UNIVERSITY OF
KWAZULU-NATAL

INYUVESI
YAKWAZULU-NATALI

E-Records Security Management at Moi University, Kenya

By

Carolyne Nyaboke Musembe
(BSc.IS, MSc)

A Thesis Submitted in Fulfilment of the Requirements of Doctor of Philosophy (Information Studies) in the School of Social Sciences, College of Humanities, University of KwaZulu-Natal, Pietermaritzburg Campus, South Africa

Supervisor

Prof. Stephen Mutula

August 2019

DECLARATION

I, Carolyne Nyaboke Musembe, declare that:

i. The research reported in this thesis, except where otherwise indicated, is my original research.

ii. This thesis has not been submitted for any degree or examination at any other university.

iii. This thesis does not contain other persons' data, pictures, graphs or other information unless acknowledged explicitly as being sourced from other persons.

iv. This thesis does not carry other persons writing unless acknowledged explicitly as being sourced from other researchers. Where other written sources have been quoted, then:

   a) Their words have been written, but the general information attributed to them has been referenced.

   b) Where their exact words have been used, then their writing has been indented and referenced.

v. This thesis does not contain text, graphics or tables copied and pasted from the internet, unless expressly acknowledged, and the source being detailed in the argument and the referencing sections.

Student Name: Carolyne Nyaboke Musembe

Date: 23rd August, 2019

Signature: [redacted]

Name of S[redacted]pervisor: Prof. Stephen Mutula

Signature: [redacted]

ABSTRACT

E-records are vital for the operation of the state as they document official evidence of the transactions of a business, government, private sector, non-governmental organizations, and even individuals. Therefore, e-records generated in organizations and institutions including universities in Kenya are considered a vital resource used as a tool for the administration, accountability, and efficient service delivery. Despite the importance of records to the growth and sustainability of any organization, e-records security management at Moi University seemed to be not well established thus exposing the records to among others, unauthorized access, risks of alteration, deletion and loss and cyber security threats. This study sought to investigate e-records security management at Moi University in Kenya. The following research questions were addressed: How are e-records created, maintained, stored, preserved and disposed? How is security classification of e-records process handled to facilitate description and access control? What security threats predispose e-records to damage, destruction or misuse and how are they ameliorated? What measures are available to protect unauthorised access to e-records? How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved? What skills and competencies are available for e-records security management? The study employed pragmatic paradigm using embedded case study research design. The target population for the study was one hundred and forty five (145) respondents consisting of top management, deans of schools and directors of Information Communication and Technology as well as Quality Assurance directorates, action officers, records managers and records staff. A complete enumeration of the population was taken, therefore a choice of sample size was not necessary. The data was collected using interviews and questionnaires. The questionnaires were administered to action officers, records managers and records staff, while interviews were administered to top management, deans of schools and directors of Information Communication Technology as well as Quality Assurance directorates respectively. Qualitative data was analysed thematically and presented in a narrative description, while quantitative data was organized using Statistical Package for Social Sciences (SPSS version 24) and summarized by use of descriptive statistics such as means, frequencies, and percentage for ease of analysis and presentation by the researcher.

The findings of the study revealed that university core business functions of teaching, research, and outreach services generated massive e-records. However, the management of such records was compromised largely because of the lack of integration of e-records management into the business process. Besides, the university lacks an e-records management programme. Moreover, there is lack of policy framework; thus, hampering e-records security management. Security of the e-records were also compromised because this activity was left until the last stage of the e-record with minimal priority. There was also lack of guidelines on e-records classification. The findings revealed challenges related to cyber-attacks, non-adherence to ethical security values, and inadequate skills that affected e-record security management. The study recommended the development and implementation of a records management programme and policies, adoption of relevant standards, developing skills about the cyberspace, provision of adequate budget, education and training.

ACKNOWLEDGEMENT

I wish to thank the Almighty God for his blessings, and for granting me good health and strength.

This thesis would not have been possible without the immense, incredible, tireless sacrifices of my Supervisor Professor Stephen Mutula. Your constant support and patience, mentorship and invaluable advice, throughout the research study made it a success. Thank you for not giving up on me my incredible mentor. May God continue to bless you.

I am forever indebted to my husband James Onyango for the selfless financial, moral and spiritual support during my study. Your unconditional love, your commitment and efforts, encouragement, sacrifices, and input into this study, inspired me to keep going despite the challenging circumstances. Thank you, God bless you.

My sincere thanks to my parents and my parents-in-law, my siblings for their encouragement and support both spiritually and morally. Your encouragement helped me pull through the study. May you live to enjoy the fruits of this work.

I thank my fellow students at the University of KwaZulu-Natal who made me feel at home away from home. Thank you to Dr. Sellah Kisaka who prepared and planned my stay, Elizabeth, for your encouragement and support and the Kenyan fraternity at the University for your Support. To my friend and year mate Everlyne Anduvare thank you for your encouragement and support. The frequent discussions and consultations we shared meant a lot. Thank you.

My appreciations also go to the Moi University staff for their precious time in accepting and providing valuable data that led to the success of this study. To Benson, Dina, Gladys thank you very much for helping in collecting the questionnaires.

Thank you all for letting me follow my dream!

Everything Worthwhile is Uphill!

Dr. John Maxwell

DEDICATION

I dedicate this work to God the giver of life; to my husband James and our Angel who begun this journey with us but couldn't live to witness the beautiful completion. We adore you.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ACRONYMS

ARMA	American Records Management Association
CCTV	Closed Circuit Television
CDs	Compact Disks
CIA	Confidentiality, Integrity, Availability
DIRKS	Designing and Implementing Recordkeeping Systems
DoD	Department of Defense
DVDs	Digital Versatile Disks
ERM	Electronic Records Management
ESARBICA	Eastern, Southern Africa Regional Branch of the International Council on Archives
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information Communication Technology
IFMIS	Integrated Financial Management Information System
IPPD	Integrated Payroll and Personnel DatabaseIRMT: International Records Management Trust
ISO	International Standard Organisation
KEBS	Kenya Bureau of Standards
KPMG	Klynveld Peat Marwick Goerdeler, Kenya
MMR	Mixed Method Research
MoReq	Model Requirement for the management of Electronic Records
NACOSTI	National Council of Science, Technology an Information
NARA	National Archives and Records Administration
PDFs	Portable Document Format
Ph.D	Doctor of Philosophy
PH	Parkerian Hexad
RC	Records Continuum
TAHO	Tasmania Archive Heritage Office
UK	United Kingdom
UKZN	University of KwaZulu Natal
UPS	Uninterrupted Power Supply

USA:	United States of America
US-CERT:	United States Cyber Emergency Response Team
WaterISAC:	Water Information Sharing & Analysis Center

CHAPTER ONE

BACKGROUND TO THE STUDY

1.1 Introduction

E-records are vital for the operation of the state as they document official evidence of transactions of businesses, government, the private sector, non-governmental organisations, and individuals. Egwunyenga (2009) points out that recordkeeping occupies a strategic position in the efficient and effective management of the University system. It is the central nerve in the administration of institutions because it documents the planning and implementation of the appropriate course of services allowing proper monitoring of work. Records are therefore useful for all organisations in management, accountability, operational continuity, legal evidence and disaster recovery (Kemoni and Ngulube 2007; Wamukoya 2009). To guarantee the usefulness of records, a series of activities which include the creation, distribution, use, maintenance, storage, security, and disposal of recorded information maintained as evidence of business transactions are essential in e-records management (ISO 2001; Bigirimana, Jagero, and Chizema 2015).

The International Standard Organization (ISO) (ISO 2001) defines a record as information created, received and maintained as evidence by an organisation or a person in pursuance of a legal obligation or the transaction of business. Similarly, Record Life Cycle and the Records Continuum Model define records as documented information, born (created or received) during a business process or activity. Shepherd and Yeo (2003) note that records may be created either in the course of an activity or afterwards in a conscious act of recordkeeping. The process of creating and receiving records may also happen when officials discharge their daily or administrative duties (Xiaomi 2003; Government of South Australia 2010).

In developed countries, the 1980s was the decade which saw a series of technological advances in hardware and software which included digital scanners, improved computer speed, low cost digital storage, image displays and laser printers all which made e-records possible and led to the development of the first records management software (Macleod and Hare 2010). However, in recent past, organisations worldwide are increasingly adopting Information Communication Technology (ICT) platform in conducting their business activities. As a result, e-records creation has quite literally exploded (Kalusopa 2011; Mutula 2013; Macleod and Hare 2010; Mcleod 2008).

A study carried out by Archives and Records Managers, and Administrators (ARMA) in 2008 found out that 90% of the records in organisations were produced in the electronic environment (ARMA 2008). The proliferation of electronic records is a consequence of the increasing use of ICTs in organisations. It brings with it the security risks of unauthorised access, loss, alteration, erasure, and damage; thus, compromising the principles of good corporate governance especially integrity, accountability, and transparency. Wagers (2010) asserts that the complex characteristics of e- records and the rapid changes in the hardware and software used to access them makes these requirements even more challenging. Grants (2014) explains that e-records have a more complicated lifecycle than a non-electronic record, because of the system issues associated with e-records. For instance, once a record is created, it must be captured by either imaging the record or importing it electronically. The electronic records must be migrated, meaning the application must be able to transfer digital materials from one hardware and/ or software configuration to another. Hence, security of e-records should begin at the creation or even before creation and should continue throughout the e-records life cycle. Massachusetts Public Records Law (n.d.) defines e-records security as the minimisation of unauthorised addition, modification, alteration, erasure or deletion of e-records and ensuring only authorised personnel to have access to the records. It also includes the policies, procedures and technical measures used to prevent unauthorised access alteration, theft or physical damage to information (Ngoepe et al. 2013; Laudon and Laudon 2005). For many organisations, security of e-records is the most critical aspect of dealing with protection of its intellectual property, trade secrets, personal identifiable information or other sensitive information. The integrity, authenticity, confidentiality, control, availability of e-records rests on the ability to demonstrate that the e-records have not been tampered with or accessed by unauthorised personnel (Kabata 2013; Bey 2012; Parkerian model 1998).

National Archives of Australia Digital Recordkeeping Guidelines (2004) defines ‘digital records’ as word processed records, spreadsheets, multimedia presentations, email, websites, and online transactions. The National Archives of Australia (2014) on the other hand defines digital records as records created, communicated and maintained utilising computer technology. They may be born digital created using computer technology, or they may have been converted into digital form from their original format, for instance, scanned paper documents. Wamukoya and Mutula (2005) define e-records as the recorded information, documents or data that provide evidence of policies, transactions and activities carried out in e-government and e-commerce environment. In this regard, e-records may be any combination of text, data, graphics, images, video or audio information that is created, maintained, modified or transmitted in electronic form by a computer or related system (North Dakota information technology department 2013). Kemoni (2009) adds that sources of e-records range from desktop publications, such as word, excel and email to corporate applications such as financial systems, human resource systems, and corporate databases. In the context of this study, electronic records mean the digital records, created, used, maintained, stored and disposed by and through computers as well as computer/digital technologies in governmental institutions.

IRMT (2009) explains that e-records must be viewed as logical rather than physical entities because they cannot be read directly without the aid of computer software and hardware to interpret the codes used to represent letters, numbers or figures. As logical entities, the three properties that are necessary to ensure the maintenance of the essential characteristics of e-records are: content (the information contained in the record); context (the intended use, purpose and recipient); structure (the appearance and physical structure) which give electronic records meaning over time and ensure efficient access (Kemoni 2009; IRMT 2009).

The records lifecycle model documents the steps in the management of records in manual form while, the Records Continuum model focuses on the management of electronic records (Edith Cowan University 2002; IRMT 1999; Upward 1997). Records generated electronically must be carefully managed through systems that provide constant intellectual and physical control. According to Technology Excellence in Government (2000), there is probably no business process that generates more interactions between information technology (IT) interests and functional managers than management of e-records. This is one of the areas of governments that has attracted the most automation and yet remains the least automated. Kalusopa (2011) asserts that it is the user's acceptance and use of its ICTs that defines its success or failure and that the integration of ICTs in records management functionalities is critical for effective and efficient e-records readiness in the organisation. Thus, e-records provide evidence of the effective operations of an organisation and should therefore be managed to ensure proper and efficient identification, storage, protection, retrieval, retention and disposal (ISO 2008).

Properly maintained and managed e-records assures good governance in government and non-governmental institutions for they are an essential ingredient to the survival of an organization because they deliver transparency, accountability, and security of information which are required for good governance (Willis 2005). Mullon (2004) observes that almost all services rendered by the government are highly depended on records. This implies that government institutions need to have effective and efficient e-recordkeeping systems to help meet user's needs. For instance, governments rely upon policy files, budgets, accounting e-records, procurement e-records, personnel e-records, tax e-records, election registers, and property fixed assets registers to demonstrate accountability to its citizens. Furthermore, for government to assure protection of entitlements of its clients, it depends on the pension records, social security records, land records, birth and death records. In addition, to enhance good governance, government has to maintain foreign relations and international obligation treaties, correspond with nationals and international bodies' loan agreements among others (Piggott 2002).

Moreover, Shepherd (2006) posits that governments use records to support accountability when they need to prove that they have met their obligations or complied with the best practice or established policies. He further reiterates that records which are managed as part of an appropriate records programme will help the governments conduct business in an efficient, accountable manner, deliver services consistently, support managerial decision making and transparent policy formulation in ensuring continuity in policy execution, management, and administration.

Effective and efficient e-records have been linked to quality service delivery (Musembe 2015; Mampe and Kalusopa 2012; Shepherd 2006). Quality service delivery begins with properly managed e-records, this is because organisations both private and public, and institutions of any size and capacity can only take appropriate actions as well as make correct decisions if they have sufficient, well managed and relevant information (Musembe 2015; Mampe and Kalusopa 2012; Ngoepe 2008). As mentioned earlier, e-records provide documentary evidence for organisational and societal use, decision making and legal use. Consequently, acceptance of e-records in legal transactions is now much more common (Maseh 2015; Shaw and Shaw 2006). E-records used as evidence in a court of law must therefore show and demonstrate a chain of accountability and custody trail. The generation of such records must also demonstrate the origin or creation through to its initial or primary use (Shaw and Shaw 2006).

Worldwide, e-government is being pursued to enhance and transform relations with citizen, businesses and other arms of government by government institutions for better service delivery. Such e-government processes create, maintain and use e-records (World Bank 2005). Chadwick and May (2003) explain that the concept of e-government first emerged in the most technologically advanced western countries including United States of America (USA), United Kingdom (UK), Canada, Australia which were also the pioneers in the adoption of the Information Communication Technologies (ICTs). These countries have also dedicated and made tremendous strides in e-records policy and guidelines development, practice and scholarly contributions. These countries appreciate e-records as an essential infrastructure for e-government and which must be effectively managed (National Archives of Australia 2014; White house 2011; UK Public Records Office 2008; National Archives and Records Administration (NARA) 2006). Similarly, African countries have not been left behind in attempting to implement e-government. They are aggressively pursuing ICTs and e-government initiatives though there are significant gaps in e-records management, in areas such as policy, reliable telecommunication infrastructure, skills and competencies (Mutula 2013; IRMT 2011b). IRMT/IDRC (2011) asserts that, while records are fundamental to the success of ICT and e-government initiatives, ICT systems will fail if e-records cannot be identified, retrieved and used, and if their integrity cannot be established.

Furthermore, e-records has been linked to the ultimate success of open government (Wamukoya 2013; Miller 2003). E-records and the evidence they provide are the means by which both private and public governments can promote a climate of trust, authentic, accurate, readily available and an overall commitment to openness. Wamukoya (2013) concurs that recordkeeping provides the means through which the creation, capture, availability, and usability of accurate, reliable and trustworthy records is guaranteed as evidence of open government initiatives.

New and emerging Information and Communication Technologies (ICTs) such as cloud computing, content management systems, social media platforms, corporate databases, web technologies, mobile platforms, Integrated Personnel and Payroll Database (IPPD), and Financial Management System (FMS) provide great potential for improving efficient management of e-records as the evidentiary base upon which organisations' governance depend (Mampe and Kalusopa 2012; Katuu 2012a; Luyombia 2011; Mnjama and Wamukoya 2007; Wamukoya and Mutula 2005). These systems specifically perform or assist in the performance of the different business activity or function, capture and manage e-records resulting from that function or activity. The success of the system depends not just on inputs and outputs, but also on the technological framework in which the system operates. Planning e-records security management programmes and ensuring a robust information architecture environment involves understanding the nature of and strength and weakness of ICT infrastructures. This also involves establishing strategies and procedures to ensure e-records are secured in the event of hardware and software damage or failure. Besides, critical success factors to the e-records system include but is not limited to adequate power supplies, robust networks, sufficient bandwidth, suitable technical support and effective backup systems (Ngoepe 2015; IRMT 2009; Mishra 2011). In addition, according to ISO/IEC 27009 (ISO 2014), the system should also allow an organisation to satisfy the information security requirements of customers and other stakeholders, meet the organisation's security objectives, comply with regulations and legislation, and also manage information assets in an organisation in a way that facilitates continual improvement and adjustment to current goals.

In addition, organisations need the policies and guidelines to rule and guide employees on records security management related issues (Asongwa 2012; Marutha and Ngulube 2012; Sichalwe et al. 2011; Ngulube 2010). This is because, in academic institutions, staff and students are increasingly creating and accessing e-records, course materials, online assessments, emails, and research databases to mention a few, that require security (Kyobe et al. 2009). Wamukoya and Mutula (2005) assert that effective e-records management can help improve service delivery, enhance accountability and transparency in governance. They point out that e-records which is not communicated is valueless. Similarly, e-records that cannot be found is worthless (Robek et al. 1996). E-records must be secured physically and intellectually throughout the life cycle to ensure that they survive for as long as they are needed to serve their purpose as evidence and information of past and present activities (Tshotlo and Mnjama 2010). For an organisation to capture and maintain accurate, complete, reliable, accessible and usable e-records, the security management of e-records is paramount to enable the institution or organisation meet its legal, evidential, accountability and cultural requirements (University of Nottingham 2015).

The new information and communication technologies have provided expansive opportunities and security threats in e-records activities. Therefore, e-records security management is expected to begin at the creation or even before creation and should continue throughout e-records life. In this regard, understanding the business functions of an institution or organisation may provide a systematic framework for e-records security management (ISO 2001). In light of the foregoing, different institutions apply strategies and procedures that include security policy, access controls, security classification, business activity classification, training and regulatory compliance that ensures minimisation of unauthorised addition, modification, alteration, erasure or deletion of e-records, ensuring only authorised personnel have access to the records and training (ISO 2001; ISO 2005; Massachusetts Public Records Law n.d; Mishra 2011).

This may enable confidentiality, availability, authenticity, integrity, and utility to be achieved in e-records security management (Parkerian model 2002). Wamukoya and Mutula (2005) assert that inadequate security and confidentiality controls are significant factors contributing to the failure of capturing and preservation of electronic records in eastern and southern African education institutions.

NARA (2006) and Massachusetts and Public Records Law (n.d.) assert that institutions and organisations' have to ensure they implement and maintain an effective security programme that incorporates the following e-records security goals: ensuring that only authorised personnel have access to e-records, backup and recovery of records are protected against information loss, staff are trained in how to safeguard sensitive and classified e-records, risk to unauthorised alteration or erasure of e-records is minimised and that e-records security is included in computer systems security plan. Furthermore, University of Nottingham (2015) states that securing services involves protecting the campus network from unauthorised access, e-records loss, identity theft, damage to computers or network services and computer viruses. Staff can in practical ways contribute to a secure working environment by applying strong passwords, not sharing their passwords and keeping such passwords safe.

1.2 Moi University

Moi University is one of thirty-one (31) public Universities in Kenya (Ministry of Education Kenya 2017). It was established as the second University by an act of Parliament, the Moi University Act of 1984, which has since been repealed by the Universities Act, 2012. The University comprises fourteen (14) schools, which include: Information Sciences; Engineering; Physical and Biological Sciences; Business and Economics; Arts and Social Sciences; Education;

Aerospace Sciences; Tourism and Events Management; Agriculture; Medicine; Law; Nursing; Dentistry; and Public Health. The University also has several directorates including Institute of Gender Education Research and Development (IGERD), Open & Distance Learning, Quality Assurance, Information Communication and Technology (ICT), Private Sponsored Students Programme (PSSP), and Internal Linkages. The University also operates the following satellite campuses spread around the country namely: Coast Campus (Mombasa County), Nairobi Campus (Nairobi County), Kitale Campus (Trans Nzoia County), Odera Akang'o Campus (Siaya County) and West Campus (Uasin- Gishu County). The University offers diverse academic programmes at undergraduate, masters and doctoral levels. It currently has a student population of over 47,000 and 3,000 academic and administrative staff (Moi University Strategic Plan 2015/2016-2020/2021).

1.2.1 E-Records security management at Moi University

Moi University has experienced phenomenal expansion since its inception in 1984 regarding physical infrastructure and enrollment. This has resulted in an increased generation of both official print and electronic records (Musembe 2015; Erima 2013). Such records include but are not limited to admission records, examination records, staff records, minutes of meetings, academic records, administrative records, accommodation records, finance records, medical records, students funding records, and more. Most of these records are generated and stored in computer process-able form in disparate systems that include, Examination Management and Financial Management System (FMS) and Hostel Booking System (SHBS). The computerized systems are embraced in most organizations to enhance among others increased productivity, greater efficiency and improved quality service delivery and support to clients through e-records management. Possibly, they allow proper capture, storage, manipulation and management and faster access to e-records due to robust searching capabilities of the e-records therein. The systems software's should provide features that augment e-records management for instance regulating the creation, usage, and maintenance, it should also enhance filing, storage, retrieval and updating electronic records. Furthermore, tracking the locations and contents of files, destruction of electronic records and making them irrecoverable, and also monitoring and controlling the destruction of e-records. This is acknowledged by Mutula (2013) citing UN e-government survey 2008, stating that increasingly more countries worldwide are using ICTs to provide information to their citizens with e-consultation and e-decision making services.

Nasieku (2010) explains that Moi University is increasingly becoming part of the digital world and consequently, e-records is becoming a reality as the use of computers as information management tools are being embraced by schools, departments and administrative offices. Therefore, security of e-records should be of paramount importance to Moi University, since records are strategic and operational assets vital for business continuity of the institution (ISO 2000).

1.3 Statement of the problem

E-records generated in organisations and institutions including universities in Kenya are considered a vital resource used as a tool for the administration, accountability, and efficient service delivery (Public Service of Kenya 2010). Despite the importance of records to the growth and sustainability of any organisation, e-records security management at Moi University is not well established, thus, exposing the records to among others unauthorised access, risks of alteration, deletion, and loss among others. This compromises on among others the integrity, confidentiality and reliability of e-records and on the operations of the university. In addition, despite the fact that Moi University has in place an elaborate information and communication infrastructure that include campus-wide management information systems comprising records units; corporate databases; Examination Management System; Hostel Management System; Financial Management System (FMS); institutional repositories; portals; email systems and internet connectivity among others, security of e-records remains the most significant concern (Musembe 2015).

An analysis conducted by Musembe (2015) on the quality management system of records in the Dean of Student Affairs, Human Resource, Financial Services and Central Registry System at Moi University revealed that the existing records system was ineffective in ensuring the security of the records. Musembe further noted that records management at the University was not well developed, thus, undermining the security of records. Musembe recommended the need for an improved mechanism of records management practices.

Similarly, a study carried out by Erima (2013) on aligning records and risk management with business process at Moi University focusing on general records management, concluded that the poor state of records management had contributed to inefficiencies in the business process exposing the University to financial risk, operational risk, and compliance risk among others. The author recommended that the University adopt a comprehensive records management and risk management programme.

A report on the implementation of ISO (2008) Quality Management System at Moi University revealed poor records control (poor record keeping affecting the security of records, poor filing, non-folioing, non-labeling) as recurring weaknesses. Despite most studies on records management at Moi University having been carried out, they have primarily focused on manual records at the expense of e-records security management.

By investigating e-records security management at Moi University, this study hopes to contribute towards creating awareness about e-records security management discourse at Moi University; providing a platform for processes, controls, policy and regulatory regime for e-records security management in order to enhance integrity, accountability, transparency and ethical conduct in records management; and also provide a framework for staff training and infrastructure development to improve e- records security management at the University.

1.4 Aim and objectives of the study

The main aim of this study was to investigate e-records security management at Moi University. The broader issues studied alongside the research questions included e-records management, records security, and information management.

The study addressed the following specific research objectives:

i. To examine the process of e-records creation, maintenance, storage, preservation, and disposal.
ii. To investigate the security classification of e-records process handling to facilitate description, control, disposal and access.
iii. To explore the security threats predisposing e-records to damage, destruction or misuse and how they can be ameliorated.
iv. To assess the measures used to protect unauthorised access to e-records.
v. To establish how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records is achieved.

vi. To find out skills and competencies available for e- records security management.

1.5 Research questions

The study, therefore, sought to address the following research questions:

i. How are e-records created, maintained, stored, preserved and disposed?

ii. How is the security classification of the e-records process handled to facilitate description and access control?

iii. What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated?

iv. What measures are available to protect unauthorised access to e-records?

v. How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved?

vi. What skills and competencies are available for e-records security management?

1.6 Scope and limitation of the study

The study was confined to Moi University main campus in Kenya to investigate e-records security management. Although the University has several satellite campuses, the respondents were predominantly from the main campus.

The study experienced some limitations. For instance, the University was in the transition of getting a new Vice Chancellor after the expiry of the incumbents' term. For this reason, an action officer in the office of the Vice Chancellor was interviewed instead of the Vice Chancellor himself. Another challenge was that the Deputy Vice-Chancellor, Administration, Planning, and Development (DVC, AP&D) had been suspended from office. To address this limitation, the researcher requested the acting DVC (AP&D) who is also the substantive DVC Student Affairs (SA) to be interviewed**.** At the time of writing the proposal, the university had a total of fifteen (15) schools. However, as the University was undergoing restructuring that included consolidation and realignments, the school of human resource was absorbed by the school of information sciences and school of business and economics, effectively reducing the number of schools from fifteen (15) to fourteen (14). This had an immaterial effect on the population size. The researcher considered this reduction in population size to be statistically insignificant to impact on the research outcome as the school was now not in existence going forward. Further, the researcher was still able to reach these respondents to provide the desired information for the study from their new schools**.**

1.7 Significance of the study

The study is expected to contribute to scholarly research discourse to the field of e-records security management. The study also hopes to improve e-records security management practice and policy formulation on e-records security management at Moi University (Mitchel 2012; Creswell 1994). The study is further expected to create awareness about e-records from creation to disposal and the inherent security practices, security classification, as well as ethical values among others. The study has unearthed e-records security management shortcomings at Moi University, which if addressed will promote sound e-records management at Moi University. These shortcomings include but are not limited to lack of adherence to essential processes, controls, procedures and policies, lack of implementation of the regulatory framework, inadequate facilitation, lack of integration of e-recordkeeping functionalities with the business processes, inadequate skills and competencies and lack of a place for e-records security management in the organisational structure. The findings are expected to provide a foundation upon which the development of a policy framework on e-records security management can be predicated.

1.8 Theory

There are several models in records and information technology that are used to underpin e-records security management that include among others Records Lifecycle, Records Continuum, Records Integrated model, Confidentiality, Integrity & Availability model and Parkerian Hexad model. These models are discussed in detail in chapter two (theoretical framework). However, this study was underpinned by the Records Continuum model and the Parkerian Hexad model. The Records Continuum model presents a seamless and dynamic recordkeeping regime that transcends time and space, thus, enhancing the management of e-records for as long as they are of enduring value. The model also provides a consistent and coherent regime of management process from the moment records are created and maintained until they are disposed (Bantin 2009; Chachage and Ngulube 2006; Makhura 2005; Yusof and Chell 2000). Records continuum model is lauded as a best-practice for managing electronic records for improving responsiveness, access controls, increasing efficiency, and satisfying users' requirements (Xiaomi 2001). However, the model has been criticised for failing to put more emphasis on skills development among recordkeeping staff and only partially discusses the security of records. Therefore, it cannot be used as a stand-alone theoretical framework in this study**.** Parkerian Hexad (PH) model was used to complement the continuum model.

The PH model is an expression of a set of six components that include confidentiality, integrity, availability, authenticity, possession or control and utility. However, the hexagon in the model not only symbolises the six elements, but it also figuratively suggests that each component fits together perfectly, solving the puzzle of comprehensive information security (Ypetkova 2012; Parker 2007; Parker 2002). The model is about organisation investing in better policy writing and enforcement, procedures and methods, employee education and awareness, and improving the available technology infrastructure. The Parkerian model also concentrates on the role that people play in perpetuating against information related loss. Security is about people and forces or acts of nature such as natural disasters, and not just technology-related security threats (Parker 2010). Employees are the biggest threat to records and information; they sometimes accidentally delete files, enter inaccurate information, save or edit the wrong files. This situation calls for training and equipping employees with right skills on how to handle e-records (Bey 2012; Andress 2011). Table 1 below maps research questions to sources of data and theory.

Table 1: Mapping research questions to data Source and theory

Research question	**Theory/model**	**Variables for investigation**
How are e-records created, maintained, stored, preserved and disposed?	Records Continuum model and PH Model	Records management practices, records creation, records capture, records maintenance, records use, records storage, records disposal, records preservation.
How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved?	Records Continuum model and PH Model	e-records security, records organisation, e-records management responsibilities

Research question	**Theory/model**	**Variables for investigation**
How is the security classification of the e-records process handled to facilitate description, control, disposal, and access status?	Records Continuum model and PH Model	Security classification, records classification, records security controls, access classification, access controls
What measures are available to protect unauthorised access to e-records?	Records Continuum model and PH Model	Classification schemes, security classification, records access control, back-up, recovery measures,
What skills and competencies are available for e-records security management?	The PH Model	Training, Training programme requirements, records management skills, records management competencies, records management resources, records management awareness
What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated?	Records Continuum model and PH Model	records security threats, records threat management, threats analysis, records threats

1.9 Preliminary literature review

The literature review is discussed comprehensively in chapter three of this thesis. The literature reviewed covers both theoretical and empirical studies. The study relied on several sources which were sourced with the help of search tools such as online databases and library database encyclopedias, indexes and bibliographies (Creswell 2014; Saunders et al. 2012). The sources searched for included but were not limited to policies, strategic plans, theses, reports, academic publications, government publications and procedural documents, journals, books, and newspapers. The study reviewed the literature on various themes related to the research problem, research questions, and the theoretical framework. They include, e-records life cycle, security classification of e-records, process records handling, security threats predisposing e-records to damage, destruction or misuse of records and how they are ameliorated; measures available to protect unauthorised access to e-records; how confidentiality, integrity, availability, authenticity, control and utility of e-records is achieved; skills and competencies available for e-records security management.

The literature reviewed studies conducted in Asia, Africa, Australia, Europe and the United States of America (USA). The literature reviewed demonstrate vast empirical and theoretical studies on electronic records management and security. Furthermore, it shows that Information Communication Technologies (ICT) have given impetus to the creation and maintenance of electronic records in the organisation resulting in a myriad of benefits and challenges. The literature reviewed also reveal that for e-records to be of value, they should contain various necessary and sufficient components that include content and context. Moreover, effective e-records management system should ensure that movement and location of records is controlled in a way that any record can be retrieved when needed and that there is an auditable trail or recordable transactions (Bigirimana, Jagero and Chizema 2015; Duranti 2010; Shaw and Shaw 2006). E-records are also vital if they can be accessed, retrieved and used. They should also be reliable and authentic as evidence of activity. Thus, there are a number of factors that should be considered in the classification of records that include value of e-records to the organisation, age of the e-records, and state of obsolescence, the standards, laws and other regulatory requirements (Marutha and Ngulube 2012; Mishra 2011). Therefore, with the advancement of technology education and capacity building on how to manage, e-records have been advocated for (Eiring 2008; Wamukoya and Mutula 2005). As mentioned earlier, with evolution and continuous use of technologies in the creation and maintenance of records, organisations worldwide are facing a myriad share of challenges in e-records management. Loss of security and privacy, inadequate funding, inadequate ICT skills and competencies, the fragility of media, the absence of accurate and complete metadata, as well as rapid obsolescence of software and hardware to mention a few, have all exposed e-records to great challenges (ICA 2016; Mutula 2013; Asogwa 2012; Kemoni 2009; Nengomasha 2009; Kaekopa 2007; Kemoni 2007; Wamukoya and Mutula 2005).

There is limited evidence in literature that show concerns about e-records security management in Moi University or Kenya in general that have been addressed. This study therefore aimed at filling this knowledge gap by answering the following research questions: How are e-records created, maintained, stored, preserved and disposed? How is security classification of e-records process handled to facilitate description and control? What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated? What measures are available to protect unauthorised access to e-records? How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved? What skills and competencies are available for e-records security management?

1.10 Methodology

The detailed research methods are discussed in chapter four of this thesis. Appropriate research methodology is required to conceptualise research problems and describe the phenomena that are being investigated (Ngulube 2015). This study employed the pragmatic paradigm which is consistent with the mixed research approach where qualitative and quantitative aspects are applied (Ngulube 2015). A case study research design was employed, whereby Moi University was the focus in investigating e-records security management at the institution. The case study design gave the researcher ample room to conduct an in-depth investigation of the unit of analysis (Yin 2009).

The study population comprised respondents purposively selected from top management, deans of schools and directors of directorates, ICT staff and administrators who are referred to in this study as action officers, records staff and records managers. A census technique was used to select respondents from each stratum. Israel (2009) states that a population of 200 or less attracts the use of census. Self-administered questionnaires were administered to action officers, records staff and records managers (see appendix 1), while a semi-structured interview was administered to the top management (see appendix 2) as well as deans and directors (appendix 3), which were used as primary sources of data.

A mixed method approach was used to analyse data. On one hand, qualitative data from interviews were subjected to thematic analysis which involved coding, grouping the data into categories, as well as identifying the themes and relationships among the categories. The major themes that emerged from the data were compared to determine the pattern of association. On the other hand, the quantitative data from survey questionnaires were analysed using Statistical Package for Social Sciences (SPSS) and tabulated by use of descriptive statistics such as means, frequencies, and percentages; these were presented using graphical tools such as tables, and graphs. A pre-test was conducted at Kisii University to assist with the validation of instruments. Data collected were analysed to generate information that was used to refine the questions for respondents. The study also adapted questions from tools that have been used in previous related studies, for instance, World Bank (2002) on Electronic Records strategy. The instruments were also availed for critical review by experts in e-records management for their comments and feedback (Saunders et al. 2012; Teddlie and Tashakori 2009; Polit and Beck 2004).

The study complied with the UKZN research ethical protocol and permission was sought from the National Commission for Science, Technology, and Innovation (NACOSTI) in Kenya. In addition, permission was sought from Kisii University to carry out a pre-test study, as well as from Moi University to administer instruments and collect data. Informed consent was sought and obtained from respondents before the commencement of the study. The respondents were asked to participate in the study voluntarily and were free to withdraw at any stage of the data collection process if they so wished.

1.11 Structure of the dissertation

This thesis is organised into seven chapters (chapter one – chapter seven). The content of each chapter is briefly summarised as follows:

Chapter One: Introduction

Chapter one provides an introduction and background to the study, description of the study area, statement of the problem, research objectives, research questions, significance of the study, scope, and limitations of the study and a brief introduction to the theoretical framework, literature review, and methodology.

Chapter Two: Theoretical framework

Chapter two presents a detailed overview of theoretical frameworks/models including Lifecycle model, Confidential, Integrity and Availability Model, Records Continuum Model and the Parkerian Model.

Chapter Three: Literature review

Chapter three provides a review of related empirical and theoretical literature covering e-records management; security classification of e-records process handling to facilitate description and access control; security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated; measures available to protect unauthorised access to e-records; how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records is achieved; as well as skills and competencies available for e- records security management.

Chapter Four: Research methodology

Chapter four discusses the research paradigm, research approaches, research design, population, sampling procedure, data collection procedure, validity and reliability of research instruments, data analysis techniques, and ethical considerations.

Chapter Five: Data analysis and presentation of findings

Chapter five presents the findings of data analysis from the questionnaires and interviews using descriptive statistics.

Chapter Six: Discussion of findings

This chapter discusses and interprets the findings using extant empirical literature and theory.

Chapter Seven: Summary, conclusions, and recommendations

This chapter presents a summary of the findings, conclusion and, recommendations. The originality of the study and areas for future research are also provided in this chapter respectively.

CHAPTER TWO

THEORETICAL FRAMEWORK

2.1 Introduction

A theoretical framework is the examination of the existing or self-formulated theories or models that are related to the study to help develop new knowledge. Moseti (2015) states that a theoretical framework can be thought of as a map or travel plan to guide the research study in its quest to develop new knowledge that will contribute to practice. Barifaijo, Basheka, and Oonyu (2010) add that a theoretical framework is a logically developed, described and elaborated network of associations among concepts of variables deemed relevant to the problem situation. Besides a theoretical framework, Upward (2001) states that models are ways of seeing things. The acceptance or otherwise of theoretical models in an area like records management depends on how much contact they make with the practical consciousness of those who undertake tasks that are part of that activity.

Theories/models therefore, enable researchers to draw new conclusions, improve on the activities and go further to come up with new theories and models that suitably explain the phenomenon under investigation. Many records and information management theories and models have been developed to underpin research in records management. Kemoni (2008) explains that many records management models have been developed by institutions, archive schools, international organisations, professional bodies, as well as archives and records management scholars.

2.2 Theories/ models of Records Management and Information Technology

The main aim of this study was to investigate the e-records security management at Moi University. The study addressed the following research questions: How are e-records created, maintained, stored, preserved and disposed? How is security classification of e-records process handled to facilitate description and access control? What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated? What measures are available to protect unauthorised access to e-records? How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved? What skills and competencies are available for e-records security management?

There are several models in records and information technology that are used to underpin e-records security which includes, Records Lifecycle, Records Continuum, Records Integrated model, Confidentiality, Integrity & Availability model and Parkerian Hexad model among others. The study was underpinned by Records Continuum and Parkerian Hexad models. This is because the Records Lifecycle and Confidentiality, Integrity & Availability model were found to be inadequate, hence unsuitable for application in the study as explained in the sections that follow.

2.2.1 Records Lifecycle Model

The Records Lifecycle model was conceived in 1956 by Theodre R. Schellenberg. His view was that the life-cycle of records had a life like a biological organism which uses a birth-to-death analogy that is, records are born, live through youth and old age then die (Shepherd and Yeo 2003). The lifecycle of records begin when records are first organised, maintained and actively used by the creators; it continues as records are stored for an additional period of infrequent or dormant use in offsite records centres and ends when their operational use ends entirely; or when they are selected as archival and valuable, and transferred to an archive or declared non-archival and destroyed (Yusof and Chell 2002). For this reason, the lifecycle model is based on the idea that records become less critical as time passes. The model suggests a separation of records management responsibilities whereby records undergo three stages namely: of current records (used regularly and frequently in day to day work of an organisation), semi-current (not in use as frequent as current records, but must be retained for legal or operational reasons), and non-current records (records that are no longer required for the work of the organisation, subject to appraisal procedures for final disposal (Spiteri 2012; Mutero 2011). Newton (1989), Yusof and Chell (2000) state that the lifecycle model reflects the opinion that all records irrespective of form and purpose, pass through certain well-defined phases and each phase requires special techniques for effective control. Gill (1993) emphasises that the records' lifecycle means a movement of records in logical steps from creation, through its use, storing, retention and finally disposal. Though the model has frequently been used, in recent years as observed by Shepherd and Yeo (2003), the life cycle model has been subject to much adverse criticism. For example, it has been questioned that some records do not die but are retained indefinitely because of their continuing value (Shepherd and Yeo 2003). This means records have the capacity to endure beyond the immediate circumstances which lead to their creation (Yeo 2011). Besides, the division between stages of the life cycle in the 'three ages' model is seen as artificial, for example, records thought to be non-current may have a renewed period of currency if the activity that gave birth to them is revived.

The records lifecycle also fails to address the management of electronic records. Furthermore, the model neither allows the repetition or omission of stages, although in practice this frequently happens (Shepherd and Yeo 2003). Mckemmish (1997) as cited by Shepherd and Yeo (2003) argues that the life-cycle concept perpetuates an artificial distinction between records kept for business purposes and records kept for cultural reasons. It also perpetuates the distinction between the professional perspective of archivists and records managers; thus, ignoring the many ways in which records and archives operations are interrelated. Therefore the Records Life-Cycle concept cannot suitably be used in managing electronic records and should be replaced by a model that takes into consideration the aspect of electronic records such as a Records Continuum (Yusof and Chell 2002; Komen 2012). For these reasons, it was not used in this study.

2.2.2 The Records Continuum Model

The Records Continuum model was formulated in the 1990s by Australian archival theorist Frank Upward based on four dimensions namely: document accountable act (creation), capture, organize and physical control and four axes (recordkeeping, evidential, transactional, identity) that serve as tools for identifying states, stages, use of recordkeeping and the development of the organisations where the records are created/received and reside (Soyka 2015; Upward 1996).

Bantin (2009), Chachage and Ngulube (2006); Makhura (2005); Xioami (2003) and Yusof and Chell 2000) state that the Records Continuum model is about continuous management of records, from the moment records are created (and before creation) and maintained until they are disposed. Shepherd and Yeo (2003) concur that the Records Continuum model argues that the management of records is a continuous process where one model passes seamlessly into another. The theory is interpreted as both metaphor and a new worldview representing a technology-driven pattern shift in records management. This implies that records are managed in a continuous process as the business processes are being carried out in institutions, thus representing a multidimensional nature of recordkeeping function, and placed in a broader social, legal and technological environment.

Xiaomi (2003), using the Australian standard 4390, defines records continuum as "… a consistent and regime of management process from the time records (and before creation, in the recordkeeping system) through to the preservation and use of records. This definition implies the integration of documents, records, and archives management. Furthermore, the definition shows that continuum is not about e-records only, but about a regime for recordkeeping which is continuous, dynamic and ongoing without any distinct breaks or phases (Bantin 2001). Viewing e-record management in a continuum is, therefore, to undercut and do away with the distinction between current, semi-current and non-current records as advocated by the records lifecycle. Shepherd and Yeo (2003) and McKemmish (2007) explain that in contrast with the older view (records life cycle) that records are kept for organisational purpose during the early stages of their lives and only later come to meet the needs of broader society as archives, the Continuum Model embraces the view that e-records function simultaneously as organisational and collective memory from the time of their creation. For example, according to Upward (2000), strategies and methodologies for appraising, describing and preservation are implemented early in the e-records management process, preferably at the design stage and not at the end of the life cycle.

McKemmish (2002) observes that the best-practice mechanism behind the Records Continuum Model is the use of an integrated approach for managing records and archives with the goal to guarantee the reliability, authenticity, accuracy, usability, and completeness of records. Thus, the model has attributes of content, context, and structure to act as evidence of business continuity. Further, Upward (2000) posits that the Continuum Model enables organisations to get a bearing in such tasks as determining social and legal requirements for recordkeeping, conducting a business process, analysing, doing a functional analysis for classification system or disposal, undertaking appraisal and carrying out systems analysis including an overview of the structuring of data about records. The model also points to the widely understood need to develop interconnected methods for document creation, establish and maintain routines within which documents are captured as records and control the distancing process involved in organising documents and records. These arguments highlight the Records Continuum model's importance as a best-practice model for managing electronic records with the aim of improving responsiveness, access controls, efficiency, and users' requirements (Xiaomi 2001). For these reasons, this study is partly underpinned by the Continuum Model (see Figure 1).

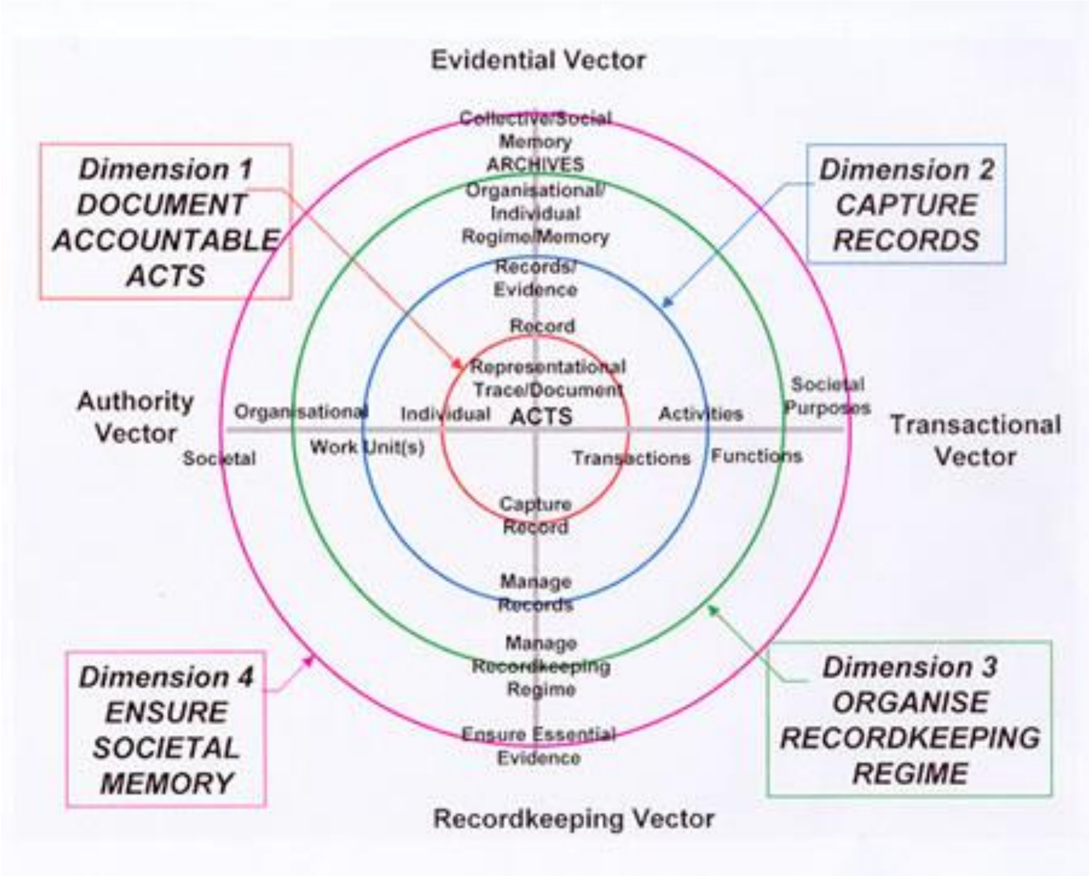

Evidential Vector
Collective/Social Memory ARCHIVES
Organisational/ Individual Regime/Memory
Records/ Evidence
Record
Representational Trace/Document
ACTS
Dimension 1 DOCUMENT ACCOUNTABLE ACTS
Dimension 2 CAPTURE RECORDS
Authority Vector
Organisational
Individual
Activities
Societal Purposes
Transactional Vector
Societal
Work Unit(s)
Transactions
Functions
Capture Record
Manage Records
Manage Recordkeeping Regime
Ensure Essential Evidence
Dimension 4 ENSURE SOCIETAL MEMORY
Dimension 3 ORGANISE RECORDKEEPING REGIME
Recordkeeping Vector

Figure 1: The Records Continuum Model (Source: Frank Upward 2001)

According to McKemmish (1997), Frank Upwards' Records Continuum model consists of four dimensions which are not boundaries; the coordinates are not invariably present; and things may happen simultaneously across dimensions. Shepherd and Yeo (2003) concur with Upward pointing out that the dimensions (create, capture, organise and societal memory or pluralise) are not time-based but represent different perspectives on the management of records. They further state that the circles move out from creation of records of business activities to ensure the records are captured as evidence and to their inclusion in formal systems for records management with the organisation, while the fourth dimension looks towards the needs of society for collective memory. The dimension of the model is outlined thus:

Document accountable act (creation): The first dimension is document accountable act (creation), which involves the identification and creation of records. This dimension emphasises the process of records creation, whether a record is managed for a split second or a millennium. These records are created as part of business activities and processes within and from outside the organisation. This also encompasses the creator(s) and players (employees, policymakers, educators/trainers, auditors, designers of recordkeeping systems and implementation strategies, consultants, advocates, standard setters) who carry out the act in an organisation (Xiaomi 2001).

Capture: The second dimension is capture, which ensures that records are captured into an effective records management system that establishes a relationship between the record, the creator and the business context that originated it. This attests to evidence of action and can be distributed, accessed and understood by others involved in undertaking business activities. Thus, it ensures that integrity, reliability, authenticity, and usability of records are achieved. Upward (2000) asserts that in the perspective of records management and the recordkeeping system of the particular work-unit, transforms the document into a record, fixing its content, context, and structure in an immutable relationship.

Organise: The third dimension is to organise or the provision of access. It involves investing the e-record with explicit elements needed to ensure that e-records are available and useful over time. This involves access, retrieval, use, security control, security classification, retention and disposal scheduling (Xiaomi 2001; Upward 2000).

Physical control: The fourth dimension is about ensuring physical control and societal memory. It involves the broader social, legal and regulatory frameworks. It ensures that records can be reviewed, accessed and analysed beyond the organisation for social, legal and cultural accountability for as long as they are required. For this reason, this dimension ensures the security of records is achieved in creating offices, registry, records and archival centres, and whether the use is by its creator or researcher (Upward 2000).

Records continuum axis

Records Continuum presents a seamless and dynamic recordkeeping regime that transcends time and space, and therefore the management of e-records for as long as they are of enduring value. Thus, a record may be involved in any of the axes, depending on when it is considered and in what context. The records continuum axis of the model is outlined:

Recordkeeping axis: Represents the state of records, as it follows a record from creation to the description, then to the organisation and incorporation in a general body of information.

A record moves out to each stage, it does not lose the previous quality and individual record within the cultural memory. It is still a document that has been created and is about context, rather than the passage of time.

Evidence axis: The evidence axis-relates to records as evidence. That is, the record as trace and evidence of actions and their role in collective and corporate memory.

Transactional axis: The transactional axis includes activities, functions and purposes and use of records.

Identity axis: The creator indicates what entity records is associated with. According to the RCM, business process and activities lead to the creation of records that are captured as evidence of the activities. When the records are captured within an organisation, it generates a corporate memory.

Based on the discussion, the model provides among others an understanding of e-records and recordkeeping processes regardless of situations, as well as perhaps the most fundamental difference between the Records Lifecycle model and the Records Continuum model. While the Records Lifecycle model proposes a strict separation of records management responsibilities, the Records Continuum model is based upon integration of the responsibilities and accountabilities associated with management of e-records (David et al. 2013; Svard 2011; Luyombya 2010; Bantin 2001).

A study by Cyrille (2010) on the management of personnel records in Tanzania stated that, records are both current and historical from the moment of their creation. They are frozen in time, fixed in a documentary form and linked to the past events, as well as dis-embedded, carried forward unto new circumstances where they are presented and used. Records continuum thinking and practice focuses on logical records and their relationship with other records, their contexts of creation and use. Thus, the continuum is a map of a dynamic virtual place – which is logical, virtual or has multiple realities – and it always has been in the paper world. Because the continuum is holistic, multidimensionality can be refracted or separated into its constituent layers like a band of light.

Table 2 presents the contrast between the life cycle model and records continuum model.

Table 2: Contrast between the life cycle model and records continuum model

Model aspect	Life-cycle model	Records Continuum Model
Origins	• Evolved from the need to effectivelly control and manage physical records after world war 11	• Evolved from the more demanding need to exercise control and management over electronic records for digital era (today)
Elements of records definition	Physical entry	Content,context and structure
Major concerns in records management	• Records centered, product-driven • Focus on records as tangible physical entities, the physical existance of records and records themselves • Paper world	• Purpose-centered, process and customer-driven; • Focus on nature of records, the record-keeping process, the behaviours and relationships of records in certain environments • Digital world
Records movement patterns	• Time – based stage: records passes through stages until they eventually 'die' accept for the 'chosen ones' that are reinacted as archives. • Time sequence: records processes take place in a given sequence.	• Multi-dimensional: records exist in space-time not space and time • Simulteniously; records processes can happen at any point in the record's existance, or indeed proceed it.
Record-keeping perspectives	• Exclusive • Single purpose • Organisational or collective memory • Current or historical value	• Inclusive • Multiple purposes • Can be organisable and collective memory • Can have current, regulatory and historical value from the time of creation

Model aspect	**Life-cycle model**	**Records Continuum Model**
		simultaniously not sequentially.
Record-keeping process	- There are clearely definable stages in record-keeping and a sharp distinction is created between current and historical record-keeping	- There should be intergration of record-keeping and archiving processes
Criteria for selecting archives	- Currency or historical value	- Continuuing value including current and historical value
Time of archival appraisal	- End of records movement	- From the begging to the end
Role of Record-keeping managers	- Passive and reactive - Locked into custodial role and strategies	- Proactive post-custodian lists, - Record-keeping policy makers, - Standard setters, - Designers of record-keeping, Systems and implementation strategies, - Consultants, - Educators/ trainers, - Advocates, - Auditors.
Undertaking records management tasks	- Things are done to the records in fixed stages, in a given sequence by particular professional group. - Records managers and archivists have no business in directing what records an organisation creates; are relagated to receiving the physical objects once created.	- Intergration of business process and record-keeping processes, the tasks can happen in almost any sequence by any professional group. - Records managers have accountabilities to ensure not only the maintainance, but also the creation of evidence of the

Model aspect	Life-cycle model	Records Continuum Model
	• Fragmented and disparate accountabilities of creators, users, records managers and archivists.	purposes and functions of organisations. • Intergrated frameworks for the accountabilities of players and partners with stakeholders.

(**Source: Xiaomi 2001)**

For those who strike a chord with the Records Continuum Model among other benefits mentioned earlier and in table two, Upward (2001) proudly states that the model can be used to provide a structure for a fundamental analysis of the earliest of record-keeping systems, and it can also be used to analyse electronic businesses including record-keeping systems within and between an organisation's back office and the broader levels of organisational and enterprise control.

2.2.2.1 Application of the Record Continuum Model to this study

The Records Continuum model is vital to this study since its emphasis is continuous management of records, from the moment records are created (and before creation) and maintained until they are disposed of. It also focuses on providing sustainable recordkeeping to connect the past to the present and the present to the future. Moreover, the Records Continuum Model recognises e-records creation to disposal as part and parcel of the business process of an organisation. This study examines among others, the process of e-records creation, maintenance, storage, preservation and disposal at Moi University. The model recognises that different personnel create and maintain records not in a discrete stage, but at different points throughout the e-records existence. It also appreciates e-records through identifiable stages. However, this stages of creation to disposal at Moi University are reference points, not separate functions.

In addition, the model ensures the creation of the right e-records containing the right information, in right formats; organisation of the records to facilitate their use; systematic disposal of records that are no longer required; as well as protecting and preserving the records (Kemoni 2008). The Records Continuum Model is a best practice mechanism that describes the management of electronic and paper records, which uses an integrated approach to managing e-records with the goal of ensuring the reliability, authenticity, and integrity of records. This is vital to an institution of higher education like Moi University which has experienced phenomenal expansion in terms of physical infrastructure and enrolment that has resulted in an increased generation of both electronic and paper records. The model therefore, provides common understanding, consistent standards, unified best practices criteria and interdisciplinary approaches in record-keeping and archiving processes.

The Records Continuum Model is most suitable to help manage such records in order to improve responsiveness, increase efficiency and satisfy user requirements. According to Xiaomi (2003), the model also emphasises capturing records of evidential quality as they are created with appropriate metadata to ensure that they are accurate, complete, reliable, and usable.

The model further reminds e-records management creators and users that e-records are created and maintained for use as a result of business and administrative functions and processes rather than the end in themselves. For this reason Moi University should provide an environment that supports the e-record-keeping and security measures to enable proper creation and maintenance.

Even though Records Continuum Model promotes the management of records in all formats, it fails to address a range of aspects that are anticipated in the study, for example, it does not put more emphasis on skills development among record-keeping staff. Furthermore, it partially discusses the security of records. Therefore, it cannot be used as a stand-alone theoretical framework for this study**.**

The relevance of the Records Continuum Model can be seen in a study by Soyka (2015) on ‘records as force multiplier: understanding the records continuum’. Similarly, the study by Luyombya (2010) applied the Records Continuum in a study on a framework for effective public digital records management in Uganda, as well as Maseh (2015) in a study on records management readiness for open government in the Kenya Judiciary just to mention but a few.

2.2.3 Confidentiality, Integrity and Availability (CIA) Model

The Confidential, Integrity, and Availability (CIA) model is a fundamental security model that has been in use for more than twenty years. It focuses on three primary areas: confidentiality, integrity, and availability. It is perhaps the most well-known model for securing information (Bey 2012; Steichen 2012; ISO 2005). According to Bey (2012), technological trends such as cloud computing and storage, and electronic information to mention a few, have made protecting information a much more complex task than ever, and it is going to get harder. The global move to digitise personnel and sensitive e-records are seemingly outpacing the capabilities of the security measures that have been in place for years. The CIA model is technology-driven and lacks the attributes to describe the procedures and methods to assure the integrity, authenticity, utility of the information and how to protect confidentiality. Furthermore, it fails to focus enough on the human element and does not emphasise regulatory frameworks in the organisation (Dardick 2011). These among other reasons has led some to question whether the CIA model is an adequate model to protect today's information. Thus, the evolving nature of technology and information use has rendered this model inadequate for the contemporary computing environment. Additionally, while all the components (confidentiality, integrity, and availability) of the model are necessary areas to be covered within the analysis of a security system, they are no-longer sufficient to analyse systems that incorporate an extensive mobile/nomadic computing environment (Reid and Gilbert 2011). This model was therefore not used to underpin this study. The model is presented in Figure 2.

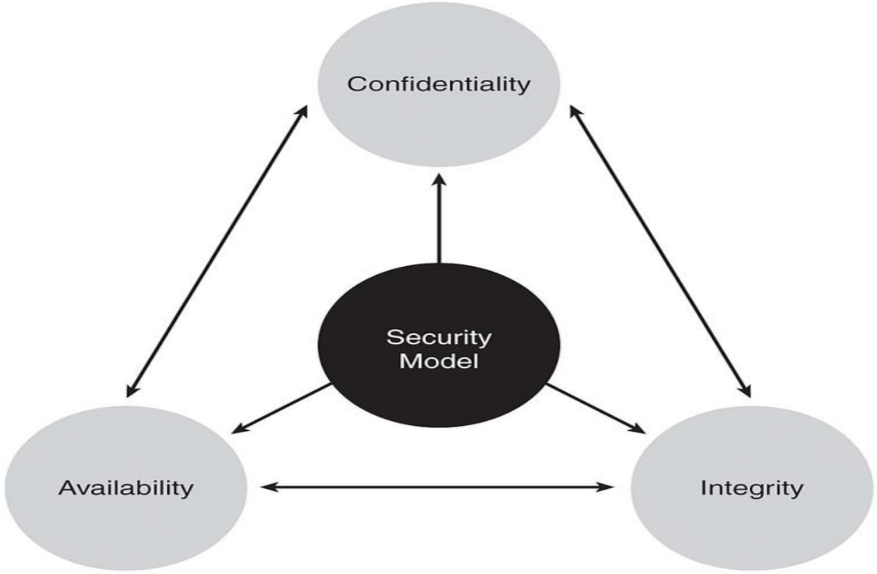


Figure 2: CIA Model (Source: Bhaiji 2008)

2.2.4 The Parkerian Hexad (PH) Model

In 1998, Donn B. Parker introduced an expanded version of CIA model which he added three elements and later renamed Parkerian Hexad (PH) Model (Bey 2012; Mishra 2011; Parker 2002). The PH is an expression of a set of components added to the CIA to form a more comprehensive and complete model (Ypetkova 2012; Parker 2007). It aimed to change how information security is understood and implemented in the contemporary computing environment where growth of nomadic computing (independence of location, motion, computing platform, communication devices and communication bandwidth where its driving dynamics include availability of hotspots, new generations of mobile phones, high demand and sale of laptops, and the increasing availability of specialised and inexpensive internet access devices) has changed the computing environment. This unprecedented level of mobile access required a new model that would in-cooperate security requirements related to a mobile computing environment as opposed to a fixed hardwired location (Reid and Gilbert 2011; Parker 2010). The six elements of PH Model include confidentiality, integrity, availability, authenticity, possession or control and utility. The PH Model is aimed at filling the gaps of the CIA model, and thus, improve the security of today's information assets. The hexagon not only symbolises the six components, but also figuratively suggests that each component fits together perfectly, solving the puzzle of comprehensive information security (Parker 2002).

In a study by Bey (2012) on the Parkerian Hexad and the CIA triad models, the author asserts that the refined security model has changed the way information security is assessed and understood. The model is about an organisation investing in better policy writing and enforcement, procedures and methods, employee education and awareness, as well as improving the available technology infrastructure. This argument is consistent with sentiments from a study by Wu (2009) on security architecture for sensitive information systems that appreciate Parkerian Hexad Model as one of the security models that is necessary to ensure information security is maintained, including that of information systems. Furthermore, the Parkerian Hexad Model concentrates sufficiently on the role that people play in perpetuating against information related loss. Security is about people and forces or acts of nature such as natural disasters, and not just technology-related security threats (Bey 2012; Parker 2010). Employees are the biggest threat to records and information; they sometimes accidentally delete files, enter inaccurate information, save over or edit the wrong files. This calls for training and equipping employees with the right skills on how to handle e-records (Bey 2012; Andress 2011). The Parkerian Hexad Model is presented in Figure 3.

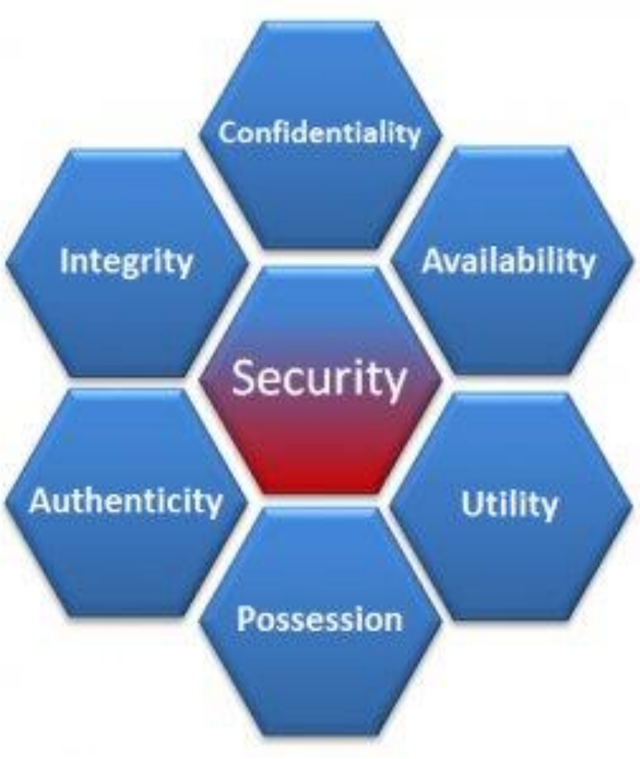


Figure 3: Parkerian Hexad Model (Source: Marzigliano n.d.)

According to Ping (2009) and Parker (1998) the Parkerian Hexad Model is non-overlapping. This means each principle (attribute) is necessary to ensure that security is maintained. The model is explained as follows:

Confidentiality: ensures that information is accessible only to those authorised to have access, prevention of disclosure to unauthorised individuals or systems (Bey 2012; Antirion 2011; Wu 2009; Bhaiji 2008; Parker 2002; Parker 1998).

Integrity: ensures that e-records are accurate and an unchanged representation of the original secure record such as transaction continuity and completeness in the business (Bey 2012; Antirion 2011; Wu 2009; Bhaiji 2008; Parker 2002; Parker 1998).

Availability: ensures that the e-records concerned are readily accessible to the authorised users at all times (Bey 2012; Antirion 2011; Wu 2009; Bhaiji 2008; Parker 2002; Parker 1998).

Authenticity: ensures the validity, trustworthiness, and dependability of e-records (Bey 2012; Antirion 2011; Wu 2009; Parker 2002; Parker 1998).

Possession (authority/ control): refers to the ownership or control ability to use e-records (Bey 2012; Antirion 2011; Wu 2009; Parker 2002; Parker 1998).

Utility: refers to the usefulness of information (Bey 2012; Antirion 2011; Wu 2009; Parker 2002; Parker 1998).

2.2.4.1 Application of Parkerian Hexad Model to this study

The PH model is relevant to the study since it strongly advocates for the security of information and appreciates the fundamental role of creators/custodians. New technological trends embraced by Moi University such as Integrated Personnel and Payroll Data System (IPPDS), Financial Management System (FMS) and Hostel booking system (HBS) among others have made e-records security and information contained therein a more daunting task. In addition, interest in e-records security has been fueled by numerous occurrences of threats, which call for better methods of securing the computers and the records they store, process and transmit — the PH model advocates for organisations to invest in better policy writing and enforcement, procedures and methods, employee education and awareness, and improving the available technology infrastructure.

Moreover, the elements of the PH Model are vital in the continuum management of e-records and necessary to e-records essential characteristics that are content, context and structure, which give e-records meaning overtime and ensure efficient access. One of the objectives of the study is to establish how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records is achieved in Moi University. Therefore, the model is vital to the understanding of the University's position on the security of e-records. Moreover, the PH Model focuses sufficiently on the role that people (e-records personnel) play in ensuring e-records security and that they are captured into an effective records management system that establishes a relationship between the record, the creator and the business context that originated it.

2.3 Summary

This chapter presented and reviewed various theoretical models that underpin records management in both paper and electronic format. The Records Lifecycle model compares a records life cycle to that of a biological organism of birth to death was reviewed. The model though widely applied, has been criticised for neither allowing the repetition nor omission of stages, although in practice this frequently happens. Moreover, the records that have non-current (death stage) may have a renewed period of currency if the activity that gave birth to them is revived. Also, the model fails to address the management of electronic records. For these reasons among others discussed, the model was not suitable for the current study. The second model reviewed was the Records Continuum Model (RCM). The RCM ensures records management is undertaken properly in a record-keeping environment built around electronic communications, which the model supports and is potentially technology-driven. It also provides for the development management systems and formulation of strategies and tactics. Its integrated approach for managing records and archives guarantee the reliability, authenticity, accuracy, usability, and completeness of records. It promotes the attributes of content, context, and structure in records.

Another model discussed that was presented in this chapter is the Confidential Integrity Availability (CIA) Model. Originally security was prescribed using the CIA model as the framework over time. It is a fundamental security model that has been in use for more than twenty years. However, the evolving nature of technology and information use has rendered this model inadequate for the contemporary computing environment. Many authors have criticised it for various reasons: it is purely technology-driven and lacks the attributes to describe the procedures and methods to ensure the integrity, availability authenticity, and utility of the information and how to protect confidentiality. The model also fails to focus enough on the human element and does not put emphasis on regulatory frameworks in the organisation. This model was not suitable for this study and was therefore not used.

The other model discussed in this chapter is the Parkerian Hexad Model (PH). The PH model is an expression of a set of components added to the CIA model to form a more comprehensive and complete model. The PH model is aimed to change how information security is understood and implemented. The six elements of PH include confidentiality, integrity, availability, authenticity, possession or control and utility. The PH model also aimed at filling the gaps of the CIA model to improve the security of today's information assets. Some of these gaps include, but are not limited to, advocating for organisations to invest in better policy writing and enforcement, procedures and methods, employee education and awareness, and improving the available technology infrastructure. The model was found suitable and was used for this study.

CHAPTER THREE

LITERATURE REVIEW

3.1 Introduction

A literature review is an explanation of what has been published or unpublished on a topic of interest by renown scholars and researchers, which is meant to provide background information and help researchers to develop a good understanding of the relevant previous publications and related emerging trends. Mathipa (2015), Creswell (2014), Serem et al. (2013), Ridley (2008), Blaxter et al. (2006), as well as Marshall and Rossman (2010) explain that in reviewing literature there is a number of benefits in a research, which include amongst others: helps in understanding the nature of the problem in order to plan the study and identify strategies needed for collecting relevant information; helps the researcher to examine the research problem from more than one angle as well as to anticipate the type of audience his/her study is out to address; provides a background to the study; assists in preparing and orienting the researcher on on-going debates, opinions and views taking place in the study; documenting how a study adds to existing literature in the field and the relationship between the present research and past researchers in the field; convincing readers that a researcher is familiar with previous works in the area of study; building readers confidence in the research work by demonstrating that the researcher has reviewed what has been done before and is not duplicating ideas or advancing far-fetched arguments; helps the researcher know what exists on the subjects and help refocus the research direction; helps find useful examples and models that can enrich the research being undertaken; have the benefit of knowing how other researchers have conducted their studies; provide a basis for understanding the importance of a study; and helps in comparing the results of the study with previous findings.

According to Creswell (2014), a good literature review follows a series of steps which include identifying key terms, locating the literature, evaluating and selecting the literature review, organising the literature, and uniting the literature review. With a cross-disciplinary nature, the study consulted several databases from computer sciences, IT and information sciences disciplines. They included but were not limited to Sage, Emeralds insight, Scopus, EBSCO, Project Muse, Research gate, Springer, Wiley, Semantic scholar, Google Scholar. Creswell (2014) recommends that when scholars conduct a computer database literature, they should consider using both free online databases and the one subscribed by the library. Likewise, the study search and selection of literature materials included standards, journal articles, thesis, and reports from e-records management and security studies conducted and published in Asia, Africa, Australia, Europe and United States of America (USA). The literature reviewed assumes that knowledge accumulates, and that people learn from and build on what others have done (Fink 2010; Sichalwe 2010; Newman 2006). To guide the search for relevant literature, the researcher used search terms including authors, subject, title, and keyword search — for instance, a combination of keyword searches such as "e-records classification", "access control", "access and classification", "e-record-keeping requirements", "electronic cyberspace", "cybersecurity", "threat assessment", records threats", "e-records authenticity", "e-records policies", regulatory frameworks", and "e-records security classification" among others that were relevant to the study. Boolean search methods were also applied in some cases to help focus and refine the search. The citations of relevant articles were noted, and attention was paid to articles and standards that were cited frequently in a variety of sources. This was done with the intent to find a broad number of articles, as well as to note those that appeared utmost significant to the study, since they were most frequently cited in a variety of sources. A significant finding from the preliminary and succeeding searches was the scarce focus on e-records security management. Although as indicated in section 1.9 that there is a vast empirical and theoretical literature on electronic records management and security that are relevant to this study, the researcher found a missing link in relation to e-records and security management. For instance, authors and scholars had sections and or/ studies on privacy and security of records management, but none had discussed the e-records security management and its themes which are intertwined, thus passing through each other seamlessly and simultaneously as discussed in this study.

Scholars have provided various types of literature reviews. For instance University of Southern California (2018), Grant and Booth (2009), Shunda (2007), Newman (2006) and Kaniki (2006) enlist thematic review (which is structured around different themes or perspectives and often focuses on debates between different schools); historical review (which considers the chronological development of the literature and breaks the literature into stages or phases); theoretical review (where an author presents several theories of concepts and focuses them on the basis of assumptions, logical consistency, and scope explanation); empirical review(which attempts to summarise the empirical findings on different methodologies); context review (in which the author links a specific study to a larger body of knowledge); integrative review (in which an author presents and summarises the current state of knowledge on a topic highlighting agreements and disagreements within it); methodological review (in which an author compares and evaluates the relative methodological strength of various studies and shows how different methodologies for example research design, measures, and samples, account for different results, whereas in a self-study review an author demonstrates his or her familiarity with a subject area).

Therefore, the researcher adopted a thematic literature review technique in presenting the literature in this study. The thematic literature review technique involved reviewing the literature related to the study organised around themes gleaned from the objectives of the study. They included: e-records management; security classification of e-records process handling to facilitate description and access control; security threats predisposing e-records to damage; destruction or misuse and how they are ameliorated; measures available to protect unauthorised access to e-records; how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records is achieved; as well as skills and competencies available for e- records security management.

3.2 E-records management

This section discusses the literature review relating to e-records management including the processes of e-records creation, maintenance, storage, appraisal and disposal and preservation that will be discussed later in this section. Many authors define e-records in different ways (Marutha 2016; Marutha 2011; Kamatula 2010; Kemoni 2009; National archives and records service of South Africa 2007; Wamukoya and Mutula 2005). In section 1.1, the researcher provides a comprehensive definition of e-records. Nevertheless, the definition of e-records is reiterated here to refer to an electronic record that can be created and/received, transmitted, or processed, maintained, used and stored by electronic means and requires some form of computer technology by an agency, institution, organisation (private or public) or individual in pursuance of legal obligations or in the transaction of business of which they form a part or provide evidence (IRMT 2009). An e-record should be what it purports to be, namely that it should have been created or sent by the person purported to have created or sent it, it was created or sent at the time purported, is complete and unaltered, is consistent and correct, and must be able to be located, retrieved, presented and interpreted for the full duration of its retention period (Lewis–Daniels 2009). In the continuum model, e-records is part of the business process of an organisation, and the process begins with records creation and the element passes to another stage of existence seamlessly

(McKemmish 1997). Consequently, e-records are subsets of information with unique characteristics in relation to other forms of information; they are results of transactions and actions, thus, must be kept reliable, authentic, available, among other characteristics discussed in section 3.2 as evidence of the particular transaction (Reed 2005; Duranti 2001). Therefore, to ensure that this subsets of information with unique characteristics are of value, (extension of human memory created from transactions and actions) and further serving the purpose of documenting transactions, communicating thoughts, substantiating claims, advancing explanations, offering justifications and improving lasting evidence (just to mention a few) to any government, organisations or institutions, proper management and security of these subsets of information should be guaranteed (Reed 2005; Cox 2001).

E-records management refers to the efficient and systematic control of creation, receipt, maintenance, use, storage, and disposal, including the process for capturing and maintaining evidence of information about business activities and transactions in the form of records in electronic format (Moloi and Mutula 2007; ISO 2001). This series of activities in e-records management enables e-records to be managed through their entire continuum from the point when the e-records are created or received through their inactive life, but have to be retained for an indefinite time for legal, fiscal, administrative or historical reasons until their disposal, which could be destruction or preservation as permanent records. Lemieux (2015) adds that, without proper records management, fraud cannot be proven, meaningful audits cannot be carried out and government actions are not open to review.

Current information communication and technological trends of cloud computing, social media, big data, biometric, and cryptography techniques to computers are having a profound impact on managing organisations' e-records (Kefron digital whitepaper 2017; Omotosho and Emuoyibofarhe 2014; Kabata 2013; Mutula 2013). In a study by Mutula and Mostert (2010) on challenges and opportunities of e-government in South Africa, they found that ICTs were critical in fighting poverty, and uplifting the socio-economic and living standard of the people in South Africa. They observed that when properly used, ICT has the potential to empower people to overcome development obstacles, address social problems and strengthen democratic institutions. These sentiments are shared in a study by Gugulethu et al. (2013) in a study on e-readiness at the National Archives of Zimbabwe. They found that the evolving ICTs have been embraced by several institutions in the country due to the obvious benefits they wish to derive from it. The authors further observed that with the adoption of e-governments, large volumes of e-records are being generated in several forms that must be properly managed and secured. These e-records become the basis for confirming pension and other entitlements, enabling and collection of taxes and census enumeration, supporting financial management and enabling audits and evaluations, helping solve land claims supporting litigation, documenting intergovernmental agreements, enabling economic planning, describing the government compliments, documenting its transgressions, monitoring the nations' development and governance and enabling other activities.

Developed countries such as USA, UK, and Australia to mention a few have made and continue to make tremendous progress in e-records management. The United States through National Archives and Records Administration (NARA) initiated the e-government electronic management records initiatives with a vision to effectively manage and facilitate access to an organisation of information in order to support and accelerate decision making and ensure accountability (NARA 2005). In 2016, NARA's federal agency through the Senior Agency Official for Records Management report indicated that 79 percent of agencies as of December 31st, 2016 are all managing emails in electronic format and 98 percent of agencies said they are optimistic about managing all permanent e-records in electronic format.

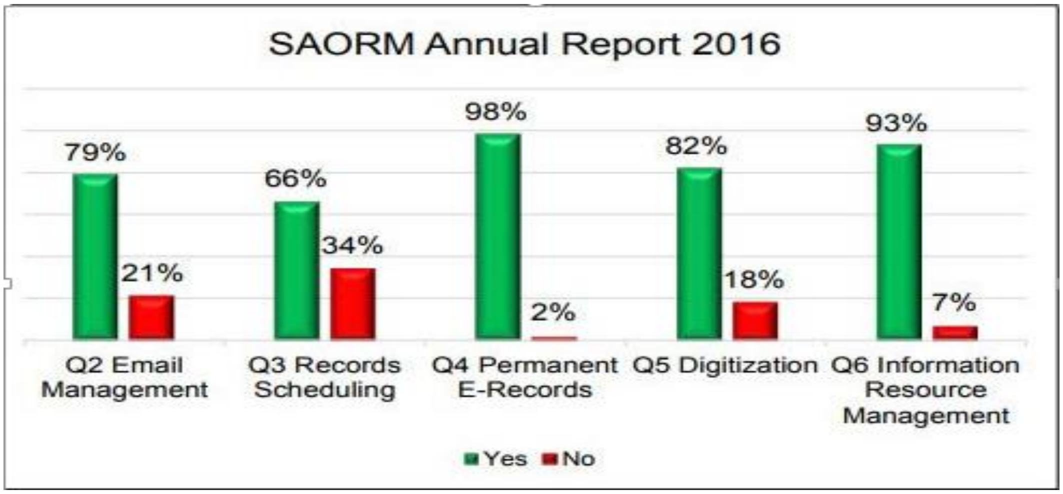


Figure 4: NARA’s federal agency through the Senior Agency Official for Records Management report (SAORM) **(Source: Federal Agency Records Management Manual 2016)**

Further emphasis is seen in NARA's strategic plan 2018-2022, which states that by the end of the year 2022, it will no longer accept the transfer of permanent or temporary e-records in analog formats and will only accept records in an electronic format having appropriate metadata. Australia on the other hand as indicated by the Library and Archives report on governance and record-keeping around the world 2018, have the goal of managing government records more efficiently with a new whole-government digital records platform developed, that will use technologies such as cognitive computing, keyword extraction, and auto-indexing to ensure that all information is automatically captured and categorised, indexed, managed and disposed.

In China, the country has faced enormous challenges in managing records in networking and digital society (Xiaomi 2009). This is seen in a report on enhancing scientific management of electronic records for China. The report notes that government authorities have faced significant challenges in managing records in networking and digital society. The report revealed that there are many problems in electronic records management of Chinese e-government. The report further notes that the functionality of national resource services was undermined due to loss of control of electronic records; the continuity of national history and memory was in danger due to loss of electronic records; the effectiveness of e-business was reduced by lack of guarantee of the legitimacy of electronic records as evidence; the protection of national security and individual rights was at risk due to issues of safety of electronic records; and e-services was not efficient due to issues of access to and use of electronic records. Reasons of the problems according to the report were paper mind; divided and separated administrative models; lack of coordination and cooperation across domains; lack of sustainable development of legal and regulatory, standard systems; and weak in research, professional education and training (Xiaomi 2009; Deng Nan 2008).

In Africa, especially in countries like Egypt, Mauritius, and South Africa, significant progress has been made in ICTs development and e-records management (Mutula 2013). Generally, most African countries have recognised e-records as inherently important to the success of ICTs integration in organisations (Mutula 2013; Wamukoya 2013; IRMT 2011). Mampe and Kalusopa (2012) citing Tale and Alefaio (2005) assert that many countries in the developing world have come to realise the importance of ICT to economic and social development, particularly where traditional systems have tended to hamper service delivery. They are of the view that the adoption of ICT presents numerous opportunities in records management such as, e-records retrieval and compact storage.

Lipchack and McDonald (2003) concur that records in electronic form are becoming especially critical as developing countries embark on e-governance strategies. These sentiments are shared by those of Nengomasha (2009), and Wamukoya and Mutula (2005) that e-records have become a very topical issue as most governments have adopted e-governance; thus, resulting in the generation of a great number of records in electronic form. Unfortunately, unlike most developed countries that embraced proper planning in development and implementation of ICTs and e-records management, authors have raised a number of issues including lack of proper planning in use of ICTs in governance (Ambira 2016; KNADS 2014; Namande 2014; IRMT 2011; Kemoni 2009).

According to Rehbein (2013), in a study on e-records management strategies, the author states that e-records come in a variety of shapes and sizes. The author further goes ahead to pose a question to organisations if they surely know what they are managing as depicted in the figure 5.

What ARE You Managing?
DVD
Dropbox
http://www.
android
SOFTWARE
LinkedIn
foursquare
LIVEJOURNAL
vimeo
YouTube
facebook
twitter
flickr
tumblr
yelp

Figure 5: What are you managing? (Source: Rehbein 2013)

Perhaps, government organisations and institutions should understand what they are managing and from what business functions the e-records are a product of. Thus, analysis of business activities and processes carried out are essential to provide an understanding of the relationship between the organisation's business and its e-records. In managing e-records in their continuum, the United States Environmental Protection Agency (2013) is of the opinion that, the systems for managing electronic records should be able to distinguish records from non-record, identify the retention and disposal schedule, allow for the disposal of records either through destruction or archiving, identify the status of the records - current, semi-current and non–current. These sentiments are shared by those of Upward (2000) (as earlier indicated in section 2.2.3), that the Records Continuum model assists organisations to understand such tasks as determining social and legal requirements for record-keeping, conducting a business process analysis, doing a functional analysis for classification system or disposal, undertaking appraisal and carrying out systems analysis including an overview of the structuring of data about records. Besides, there is a need to develop interconnected methods for document creation, establish and maintain routines within which documents are captured as records, and control the process involved in organising documents and e-records. Since in electronic record systems the decisions about capture and classification, access and disposal statuses are usually made at the point of creation of the record; the processes are both more explicit and usually simultaneous. The Records Continuum Model explains that the four dimensions of managing e-records (identification of records, capture, organisation or provision of access to records and their physical control) are no boundaries, the coordinates are not invariably present, and things may happen simultaneously across dimensions. (McKemmish 1997; Upwards 1991). In this regard, organisations should be able to understand the rationale for the creation, maintenance, use, storage and disposal of records having in mind that e-records management is not about e-records only, but a regime for recordkeeping which is continuous, dynamic and ongoing without any distinct breaks or phases, thus processes pass seamlessly into another as discussed in the subsequent section (Shepherd and Yeo 2003; Bantin 2001, McKemmish 2001; Upward 2001).

Records creation, receipt, and capture: according to the Records Continuum model as discussed in section 2.2.2, the creation dimension emphasises the process of records creation, whether a record is managed for a split second or a millennium (McKemmish 2005; Upward 2001). As discussed in section 1.1, e-records may include, but not limited to emails, word processing documents, spreadsheets, databases, websites, images, videos, audio, multimedia, interactive documents, and scanned/digitised documents. They include records created, sent, received by employees, appointees or elected officials of government, organisations or institutions, as well as interactions with other national or internal organisations. Consequently, e-records that have been created or received in an organisation should link to each other to enhance access and retrieval. This is because such records were created and received for use as a result of business and administrative functions and processes, rather than as ends in themselves (Xiaomi 2003).

E-records were earlier created or received on either personal computers (where individuals control the creation and use of the e-records), in shared computer servers (where individuals control the creation of records, but share those records with others in the organisation), in shared servers with centralised control (where all individuals adhere to established procedures for creating and managing records) and shared servers using electronic document or records management software (where control over the creation and use of the records is strongly regulated) (IRMT 2009). In recent years, the number of platforms that organisations use to create e-records has rapidly increased. For instance, social networking, web publishing, microblogging, blogs, wikis and file sharing/storage (google documents) and Smartphone technologies which run on applications like Apple, Android, and Windows. This smartphone technologies and platforms are used and created to connect people to governments and organisations and to share information, for example providing information on promoting discussions about the government, soliciting responses from the public, recruiting personnel and providing collaborative space work in new ways, providing interactions and collaborations among users and also the platforms are used to create, publish, reuse content, share files and host content among others (Mutula 2013; Wendy 2013; NARA 2011, NARA 2010). Unfortunately, not all content created using these smartphone technologies and platforms are necessarily qualified as e-records. According to NARA (2011), the following five questions should be asked to help determine whether particular content is a record: is the information unique and not available anywhere else? Does it contain evidence of organisation policies, business, and mission among others? Does the organisation authorise this platform? Is there a business need for the information?

In addition, the e-records created and received should meet operational policy, legal and financial purposes and document accurately and adequately the organisational or institutional functions, policies, procedures, decisions and transactions to serve as reliable evidence, for instance, in protecting the interests of the organisation and the rights of employee, clients and other stakeholders. For this reason, e-records created or received should be controlled, maintained and organised in a manner that guarantees full and accurate evidence of business activities for as long as the evidence is required (AIIM 2009).

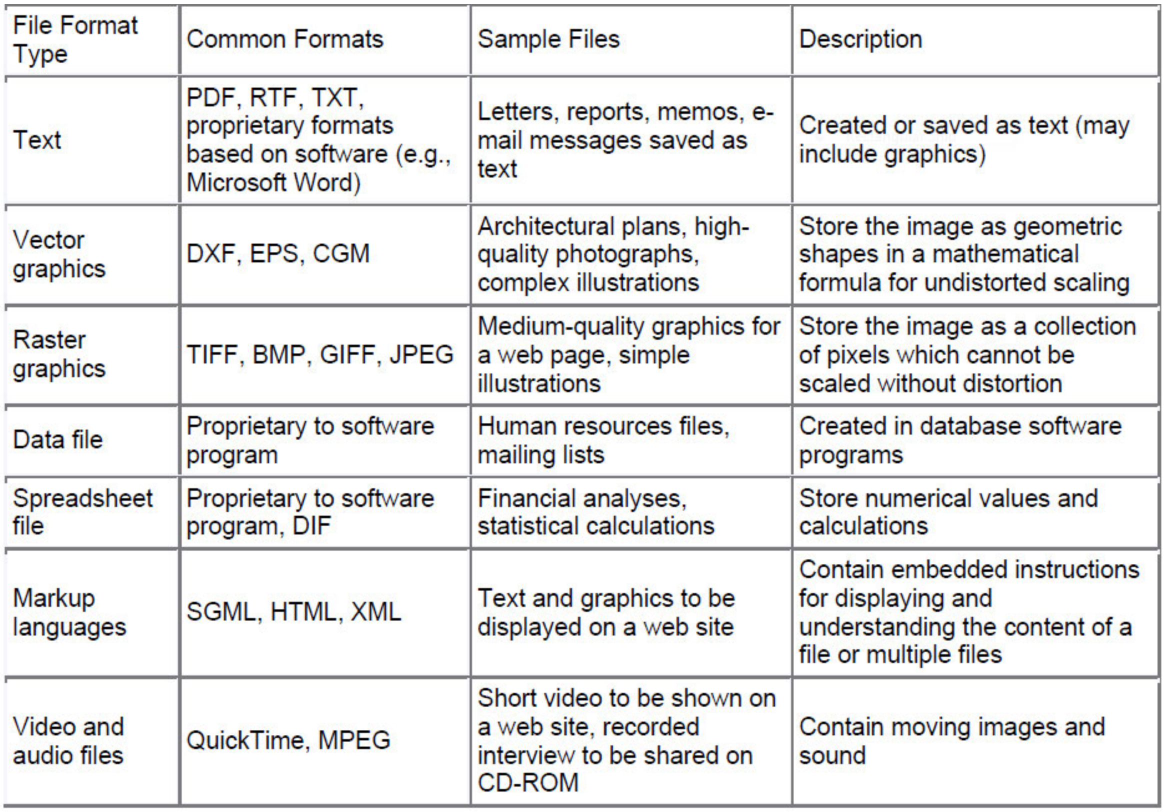
Consequently, organisations and institutions should have a systematic approach to records creation and/ receipt which incorporate e-records creation and receipt as part of organisation or institution routines. In relation to the Records Continuum Model, Upward (2000) asserts that at creation, a master plan should be developed to manage each record effectively until its disposal, since records are created as part of business activities and processes within and from outside the organisation. Thus, organisations and institutions should give clear instructions to personnel on ‘what’ records should be created or received (for instance, inward and outward communication with the internal, external persons, national and international organisations, minutes and other records of meetings, consultations and deliberations pertinent to decision making, formulation of policies and procedures, transaction of business activities, departmental forms and registers, reports, accounting documents, health records, receipts, inventory documents), ‘who' created or received the e-record (for example chief executive officers, action officers, deans, directors, county officials, national governments officials, vice chancellors, deputy vice-chancellors, principals, coordinators), ‘when' created or received (for example records should be created immediately after completion of a business process or transaction and reports or minutes of meetings written immediately after completion of the meeting or function), and ‘where' the record should be stored, which will be discussed later in this section (Eusch 2017).

Therefore, after e-records are created or received, the metadata for those particular records is captured, the purpose of capturing e-records into the system is to establish among others the relationship between the record, the creator and the business context that originated it and place the e-record within the established relationship and link it to other records (ISO 2001). In most cases, at the time of creation, e-records usually are accessible only to their creators and perhaps to the other members of a work unit. The time they are captured into the e-record management system, they usually become more accessible, and it is also the moment when the existence of the e-records is published, and it may be the point at which formal access controls are applied (as discussed in section 3.5.1), and also protecting confidentiality, integrity, authenticity among others (discussed in section 3.4) (Shepherd and Yeo 2003; Parker 2002). Consequently, referring to the capture dimension of the Records Continuum Model, Upward (2000) affirms that in the perspective of records management, the record-keeping system of the particular work unit transforms the document into a record, fixing its content, context, and structure in a stable relationship.

The Content characteristic is all about information in the record that documents organisational business activities. For instance, content can be composed of numbers, texts, symbols, data, images or sound. Thus, the information content of a record should be an accurate reflection of a business transaction or activity. Context characteristic, on the other hand, is about information that shows how the record is related to the business of the organisation and other records. Contextual information is crucial to the evidentiary functions of records. If a record lacks critical information about its creator, the time of its relationship to other records, its value as a record is severely diminished or lost entirely. Also, when organisational records are made available to its clients without context, it undermines the utility of the information and compromises its value as evidence. The last essential characteristic is the structure which is about appearance and arrangement of a records content and technical characteristics of the e-record; for example formats, data, organisation, and the relationship between fields, page, layout, style, fonts, and paragraph, breaks, hyperlinks, headers, and footnotes (Wamukoya 2013; State of Florida 2010; Moloi and Mutula 2007; Shepherd and Yeo 2003; McKemmish 2002; ISO 2001; Upward 2000). These sentiments are expanded by Duranti (2010), in her study of concepts and principles for the management of e-records at the University of British Colombia. Duranti identified and defined the necessary and sufficient components that must be captured in a digital information system when creating e-records that include medium (the physical carrier of the message), content (the message that the record is intended to convey), physical and intellectual form (the rules of representation that allow for the communication of the message), action (the exercise of will that gives origin to the record), persons (the entities acting by means of the record), archival bond (the relationship linking each record to the previous and subsequent one), and context (the judicial, administrative, procedural and documentary framework in which the record is created).

Organisations should also consider standard formats for e-records creation and capture. In most computer systems the software in which a file is created usually has a default format, which contains an extension of the software in which they were created. The standard file formats for e-records creation or receiving may include, but not limited to, Text file formats (for instance, Word document [.DOC], Rich Text Format (.RTF), text files (.TXT) and Portable Document Format (PDF), Graphic files (which store images for photographs and drawings for example Drawing Interchange Format (DXF) files used in computer aided design software programs such as those used by engineers and architects; Encapsulated PostScript (EPS) files which are used widely in many image-oriented software programs and offer high degree of durability; Tagged Image File Format (TIFF) files usable in many different software programmes; Bitmap (BMP) files used mostly in word processing applications; Graphics Image File Formats (GIFF) used for internet application and Joint Picture Expert Group (JPEG) also known as JPG files are images that have been compressed to store a lot of information in small size files); Data files (created in database software programs, which are divided into fields and tables that contain discrete elements of information; the software builds the relationship between these discrete elements for example name, address, gender and job group that may be organised into separate tables); Video and audio files which contain moving images digitised video, animation and sound records. They include QuickTime and Motion Picture Expert Group (MPEG) formats). The last possible file format used is Markup languages also called Markup formats which contain embedded instructions for displaying or understanding the content of the file. The World Wide Web Consortium (W3C) (http://www.w3c.org/) supports these standards. They include Standard Generalised Markup Language (SGML) an international standard format used in government offices worldwide. Another format is the Hypertext Markup Language (XML), a relatively simple language based on SGML that is popular for managing and sharing information (Franks 2015; Minnesota state Archives 2012; Nuclear Information and records management association technical guideline 15 (NIRMATG 2011)) as summarised in table 3.

Table 3: Standard formats for e-records creation and capture



File Format Type	Common Formats	Sample Files	Description
Text	PDF, RTF, TXT, proprietary formats based on software (e.g., Microsoft Word)	Letters, reports, memos, e-mail messages saved as text	Created or saved as text (may include graphics)
Vector graphics	DXF, EPS, CGM	Architectural plans, high-quality photographs, complex illustrations	Store the image as geometric shapes in a mathematical formula for undistorted scaling
Raster graphics	TIFF, BMP, GIFF, JPEG	Medium-quality graphics for a web page, simple illustrations	Store the image as a collection of pixels which cannot be scaled without distortion
Data file	Proprietary to software program	Human resources files, mailing lists	Created in database software programs
Spreadsheet file	Proprietary to software program, DIF	Financial analyses, statistical calculations	Store numerical values and calculations
Markup languages	SGML, HTML, XML	Text and graphics to be displayed on a web site	Contain embedded instructions for displaying and understanding the content of a file or multiple files
Video and audio files	QuickTime, MPEG	Short video to be shown on a web site, recorded interview to be shared on CD-ROM	Contain moving images and sound

(Source: Minnesota State Archives 2012)

Maintenance and Storage: Matters relating to maintenance and storage of e-records arise throughout their existence as indicated in the introduction of this section (3.2). During maintenance, e-records should have back up, system-wide backups done periodically, ensure after every transaction that the users back-up their files, and keep them off-site, as well as also ensure unauthorised persons are not allowed access to the e-records.

E-records should be stored in a manner that facilitates user access and ensures they are secured from unauthorised access, use, disclosure removal, deterioration, loss or destruction. Selection of storage media, storage system, storage environment and handling procedures should be based on e-records management and business considerations (for instance volume and growth rate of records), e-records security needs, retrieval requirements and preservation needs (The University of state of New York 2014; Government records service of Hong Kong 2011). ISO (2001) advises that suitable e-records conditions should be provided to protect the e-records from authorised access, loss or destruction mainly in the event of a disaster. According to Massachusetts Public

Records Law (n.a.), the following factors should be considered before selecting a storage medium or converting from one medium to another. They include: the authorised life of the e-record as determined by organisations e-records guidelines, the maintenance necessary to retain the e-record, the cost of storing and retrieving the e-records, the records density, the records time to retrieve stored e-records, the portability of the medium that is selecting open standard media that will run on equipment offered by multiple manufacturers.

Observing proper factors before deciding on a given storage way is vital because there are numerous ways of storing e-records; thus, inviting organisations to select wisely before settling on any. The storage ways may include, but not limited to, personal computers, shared computer servers or shared servers with centralised control, external hard drives, cloud computing, social media, smart devices (including phones), flash disks, DVDs, computer disks CDs, data centre's emails, software platforms like databases, accounting systems and websites (Rehbein 2013; IRMT 2009). Grants (2014) is of the opinion that storage plans must include online storage, which allows information to be stored on a hard drive or a server; near line storage which allows information that is accessed less frequently to be stored on disks or other medium that may not be immediately accessible; and off-line storage which allows long-term electronic records to be preserved in a vault or some other secure location.

Appraisal, retention and disposal schedules: an e-records appraisal is the analysis of all records to determine their administrative, fiscal, historical legal and other archival value that are of benefit to the organisation and its stakeholders (Maryland State Archives 2015). Ismail and Jamaluddin (2009) add that appraisal practice involves the act of making a decision on the records to be created and how long records need to be kept ensuring organisational accountability. A disposal schedule as a control document, records appraisal decisions and prescribes disposal action (IRMT 2009). Like any other records in other formats, retention and disposal periods for e-records are derived from functional needs of the organisation and any additional and audit needs; thus, appropriate appraisal scheduling and disposal procedures should be applied, so that e-records needed for either decision making or lawsuits may not be destroyed unintentionally. For example, in case of a lawsuit, should destruction actions not be appropriately documented, any destruction of e-records could be seen as a deliberate obstruction of justice (Mukwevho and Lorrette 2013; Kenya public service 2010; National Archives and Records Services of South Africa 2006). According to the

University of Cincinnati (2007), a record shall be retained for such a period as is required by the retention schedule established by the University and may be disposed only in accordance with disposal instructions issued by the University. Removal, destruction, mutilation alteration, transfer or other disposal should be carried out as per the policy frameworks available.

E-record preservation: Preservation of e-records is inextricably intertwined with the ongoing management process of e-records management the same as the already discussed processes of creation, maintenance, appraisal, retention, and disposal. E-records require specific hardware and software to ensure that they are accessible, retrievable, and understandable to users. As such, they are technology dependent and require proactive actions to preserve as long as they are required to serve as continuous business and operational needs, protect the legal, regulatory, financial and requirements, as well as interests of the organisation, their employees and the public, ensure the legal admissibility of e-records to meet evidence purposes, avoid causing damage to the damage and reputation of the organisations due to inaccessibility, un-usability or loss of e-records to demonstrate an open and accountable organisation and avoid high recovery costs to reconstruct e-records that have become unreadable, just to mention a few (Handbook of preservation of electronic records 2013). Hence, e-records preservations is one of the several activities that are carried out as part of the e-records management functions necessary to maintain the form, authenticity, integrity, reliability, usability and security as evidence of an activity.

Marutha and Ngulube (2012) in a study of e-records and medical record-keeping practice in the public health sector of the Limpopo Province in South Africa concur that e-records should be preserved in a way that its form, retrieval, reliability, and authenticity as evidence of a particular activity are not subject to change, while ensuring the safety of the e-records. They noted, for example, that if the information in the medical records is changed, it will be useless or misleading to clinicians, nurses and eventually doctors; thus, causing a health risk. However, the process must be carried out with proper planning in relation to well-run records systems (in this case policies and frameworks, standards, and regulations), technological implementations, and requisite resources. The process also requires concerted efforts of different stakeholders including records managers, ICT personnel, top management, consultants, departmental heads and other action officers who have related qualifications. Otherwise, if this process is not taken with serious consideration the e-records and the connections between them cannot be preserved systematically and much of the meaning will be lost, even with a short period of time (ICA 2016; Handbook of preservation of electronic records 2013; Beagrie and Jones 2008; Brown 2008; UK digital preservation 2008).

Organisations should come up with e-records preservation policy or approaches and strategies that will ensure that its e-records are maintained and sustained in an accessible format as long as a need for those records exists, thus, ensuring those of current and continuing value are created and maintained in a way that will both preserve their value and include appropriate access arrangements to them. This need may include corporate records, research contracts, students' records, Memorandum of understanding, personnel records, government circular among those discussed earlier in the section (Handbook of preservation of electronic records 2013; Wamukoya 2013; Upward 2006).

There are two preservation approaches used in e-records- active and passive preservation. Active involves Migration process. Planning and taking actions to offset technology obsolescence of e-records, which may involve adopting new technologies that were not in existence when the e-records were initially created (ICA 2016; Handbook of preservation of electronic records 2013; IRMT 2009; UK National Archives 2006; McKemmish 2005).

Consequently, migration process involves a change in storage media, and computer hardware, and software. For example, moving an e-records to either a new format, for example, Microsoft word 2010 to Microsoft word 2013, or another format from Microsoft word 2013 to PDF. The decision about upgrading software from one version to another or changing to software altogether should not be made without considering the implication to the e-records and their on-going integrity (ICA 2016; Dressler 2010; IRMT 2009; Beagrie and Jones 2008; Brown 2008). Figure 6 shows critical steps that can be followed during migration of e-records.

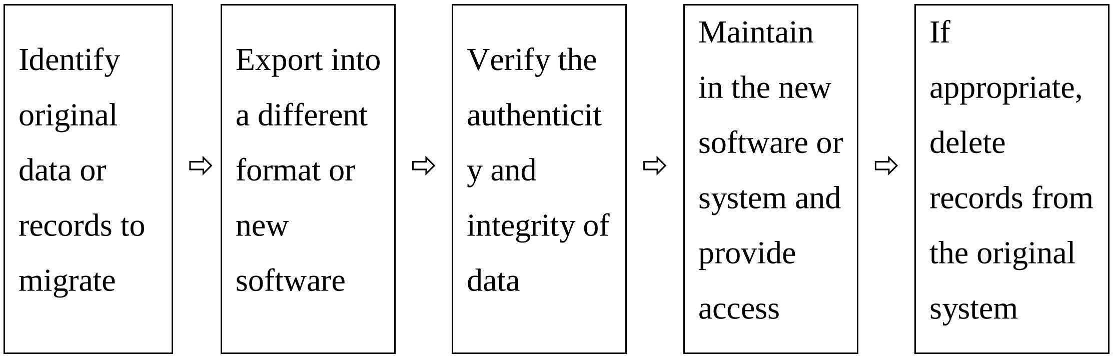

Identify original data or records to migrate
Export into a different format or new software
Verify the authenticity and integrity of data
Maintain in the new software or system and provide access
If appropriate, delete records from the original system

Figure 6: Key steps in e-records Migration (Source: IRMT 2009)

Passive preservation is the second approach in e-records preservation. It refers to the provision of secure storage and integrity of each record manifestation aiming to ‘keep' the original e-records intact without changing the technologies used to store or process it and maintain appropriate access control and securing offsite storage. Passive preservation techniques may include refreshing, emulation and encapsulation. Refreshing refers to reading and rewriting stored e-records to ensure they are retained accurately. This can take place when hardware and storage media are being upgraded to take advantage of technology advancements for instance increased storage capacity to reduce costs or to accommodate new business requirements. Emulation, on the other hand, refers to keeping the original operating system used to create and manipulate the e-record. For example, if a record was created in an IBM DOS system, an emulator (means to mimic the environment of the original of a digital or e-record) can re-create the original operating platform and software used to render the record in its original environment. Emulation is regarded as an interim measure until systems are developed that recreate the e-record, without emulation software. Consequently, specifications need to be kept describing how the original environment operated so that it can be re-created. Another passive preservation measure is encapsulation, where the e-record to be preserved should be self-describing. It ensures metadata about the record's original relationship is packaged with it to aid other preservation strategies including emulation or migration. The approach makes it possible to access e-records now and in the future using emulators, viewers, and converters (ICA 2016; Victorian electronic records strategy 2011; Dressler 2010; Gultenbrunner et al. 2010; Woods and Brown 2010; Boudrez 2005).

3.2.1 Integration of e-record-keeping functionalities into business process systems

E-record-keeping functional requirements are about the organisation’s focus on the outcomes required to ensure records are managed properly. The choices made on how the e-records are managed will influence the extent to which each organisation must consider the amendment for inclusion within a business system (Government records 2016; ICA 2008). Organisations and institutions should understand the basis for designing systems that will capture and maintain e-records and the benchmark for measuring the performance of the existing systems. Similarly, the organisation should ensure that user requirements including user acceptance are considered because such requirements are significant factors in successful implementation. The Parkerian Hexad Model asserts that an organisation should focus on their people (personnel) for they are the creators, users, and maintainers of the system. The systems should be able to link e-records to business activities, retain records of past actions and fix the content, context, and texture over time; thus, helping in maintaining records authenticity, reliability, integrity, availability, confidentiality, usability, and accessibility at any time as discussed in section 3.3 and 3.6 (National Archives of Malaysia 2011; Parker 2002; Upward 2001) .

The design, development and implementation of a records management systems may involve a series of phases. For example, the Design and Implementation of Record-keeping Systems (DIRKS) which originated from the cooperation activities between the State Records Authority of New South Wales and the National Archives of Australia that provides an eight-phase instruction including preliminary investigation, analysis of business activity, identification of record-keeping requirements, assessments of existing systems, strategies for record-keeping, design of a record-keeping system, implementation system and post-implementation (State Records Authority of New South Wales and National Archive of Australia 2001; 2003). It is worth to note that because business process and records systems are not static, the phases may be revised periodically. According to ICA (2008), designing, developing and implementing of a system commence with planning and establishment of a project charter (this phase involves but is not limited to identifying and validating an opportunity to improve business accomplishments of the organisation or deficiency related to a business need, identifying significance, assumptions and constraints on solutions to the need and recommending the exploration of alternative concepts and methods to satisfy the need), which may be initiated as a result of business improvement activities, changes in business functions or advances in information technology, or may arise from external drivers such as laws and policies, the establishment of new strategic directions for the government or the pursuit of opportunities presented by external organisations. Planning is the second phase where the needs of the system and proposed concepts for the new or modified system are further analysed in order to inform the development of a ‘vision' of how the business will operate once the approved system is implemented — other high-level requirements are those of security (that the nature of the security certification and accreditation activities and record-keeping are further refined based on threat and risk assessments). Thirdly, the requirement analysis phase is where all functional user requirements are formally defined and delineated in terms of data, system performance, security and maintainability requirements for the system. At this phase, all the requirements are defined to a level of detail sufficiency for systems design to proceed. All requirements should be measurable and testable and relate to the business need or opportunity identified in the initiation phase. Documentation related to user requirements from the planning phase are used as the basis for further needs analysis and the development of detailed user requirements. Consequently, in this phase, the system is defined in more detail concerning system inputs, processes, outputs, and interfaces. The phase also focuses on determining what functions must be performed rather than how to perform those functions.

The fourth phase called design is where the physical characteristics of the system are specified, and detailed design prepared. Here, the operating environment is established, significant subsystems which consist of inputs and outputs are defined, and processes are allocated to resources. Everything requiring user input or approval is documented and reviewed by the user. Organisations also must account for the functional requirements for record-keeping and other related requirements for instance management, procedural and technical that would have been identified in the previous requirements analysis stage. Similarly, record-keeping design specifications should be woven seamlessly into the physical and logical design specifications (inclusive of data architecture and data models for the system). The fifth phase which is implementation- the activities of this phase translate the system design produced in the design phase into a working information system capable of addressing the system requirements. The implementation phase contains activities for building the system, testing the system and conducting functional requirements qualification testing to ensure the system functional processes satisfy the functional process requirements. An important step prior to installation and operating the system in a production environment is to subject the system to certification and accreditation activities. Maintenance becomes the sixth phase where the system is monitored for continued performance in accordance with user requirements and required system modifications are incorporated. The operation is assessed if the system can be effectively adapted to respond to an organisation’s needs through in-process reviews to determine how the system can be made more efficient and effective. This means changes to the record-keeping requirements (that is driven by new laws, changing business requirements in the design of business process among others) must be accommodated in the monitoring, and change process activities undertaken during this phase. Thus, new users will require training and ensuring that user needs are met, and the system continues to perform as specified in the operational environment. When the modifications are changed and identified as necessary, the system may re-enter the planning face.

Review and evaluation, which is the last phase as explained by ICA (2008) occurs in two sub-phases. The first is the perspective of the business system itself. In-process reviews are conducted at each phase of the systems development life cycle to ensure that the activities undertaken in any given phase achieve their pre-defined goals and meet their performance targets. Such in-process reviews must be supported by agreed performance measures and assessment methods. For example, if the capability of the system to generate, capture and manage records is to be measured, then performance measures for record-keeping and methods for carrying out assessments of record-keeping capability must be developed, applied and wherever possible, integrated in the performance measures and assessment methods employed in the in-process reviews conducted at each phase of the systems development life cycle. The second perspective is the methodology employed to develop the systems- this must be effective, efficient, and complete among others. The evaluation of the methodology can occur at the conclusion of the business systems project or as part of the overall general assessment of the development and management of business systems. Again, record-keeping considerations, including performance measures and other criteria, must be developed and integrated into the tools and techniques employed to assess business systems development generally.

Despite systems being in place in many organisations, a study by IRMT/IDRC (2011) established that in ‘too many' cases ICT systems were being introduced without incorporating the essential processes, controls, and standards needed to regulate the creation, capture, access, and safeguards on a long-term basis of electronic/ digital records. ICA (2008) advices that e-records management systems must capture the content, structure, and context of e-records to ensure they are reliable and an authentic representation of the business activities or transactions in which they were created or transmitted. Moreover, e-records systems should be integrated with business applications that generate e-records, so that the records can be captured within the e-records management systems. The e-records systems should also provide for possibilities of access options to e-records offline and online (Ambira 2016). These systems which are primarily software-based methodologies used to manage e-records should also be guided by organisational business procedures and activities (Ngoepe 2014). System software may include the capabilities of integrated document management system, records information management software, document imaging system, digital repositories, electronic document and records management system (Codafile 2015; New South Wales Government 2012).

Australian National University policy (2015) and Moi University ICT policy (2011) explain that universities' systems should include among others student administration system, research data management and repository system, hostel booking management system, examination and clearance system, integrated financial management system, electronic repository, human resource management system, health records management information system, library information system, and research information system. Therefore, e-record and information systems should ensure e-records are accessible, available and always remain unchanged to enhance accountability, integrity confidentiality and control to mention a few (Omotosho and Emuoyibofarhe 2014).

3.2.2 Policies, guidelines, regulations, and standards in records management and security

Proper e-records management is practical when organisations develop and implement required legislation including laws and regulatory frameworks (for instance the constitution, computer and security acts, Freedom of Information (FOI) acts, records disposal Act), policies, procedures and/guidelines (for example e-records and information policy, ICT policy, Internet use policy, human or employee training policy and security policy), Parkerian Hexad Model advocates that organisations must invest in better policy writing and enforcement, procedures and methods, implementation of the policies and improving the available technology infrastructure (Parker 2002). Many authors have advocated the development of policies since time memorial (Wamukoya and Mutula 2005; Katuu 2005). Consequently, a worthy e-record framework consists of information–related laws, policies, and programmes, records management standards, and practices and the necessary qualified human resources to implement and manage the systems. The legal and policy frameworks ensure a strategic approach to building capacity to capture, process, store, use, conserve and preserve e-records and national heritage (Chibambo 2003).

ISO 15489-1 (2001) asserts that all organisations must identify the regulatory environment including statutes and laws that affect their activities and requirements to document their activities. Moreover, the nature of the organisation and the sector to which it belongs will determine which of these regulatory elements (individually or in combination) are most applicable to that organisation's records management requirements. On policies and procedures, ISO 15489-1 (2001) asserts that organisations seeking to place proper e-records management should document, maintain and promulgate policies, procedures, and practices for records management to ensure that its business need for evidence accountability and information about its activities is met. Furthermore, organisations' policies and procedures should reflect the application of the regulatory environment to their business processes (ISO 2001).

Macleod, Childs, and Heaford (2007) point out that the United Kingdom (UK) developed their legislation and toolkits based on the ISO standards to improve their RM as required by citizens' right of access to information, while the USA developed legislation to govern and enforce proper record-keeping after serious scandals. However, Norris (2003), reports that not many higher education institutions in the United Kingdom had well defined and active e-mail policies in place. This was also the case at the University of Loughborough. In most governmental bodies in developing countries, there is lack of or inadequate policies and other best practices to govern e-records management. Many authors lament that, even those governmental bodies that have policies, procedures or guidelines, and standards, were only available on paper or electronic format, but they are not implemented (Ngoepe 2014; Mula 2013; Mutula 2013; Nengomasha 2013; Wamukoya 2013). Wamukoya and Mutula (2005) assert that the failure of Eastern and Southern African Institutions of higher education to capture and preserve electronic records has been attributed to the lack of policies and procedures among other factors. Asogwa (2012) concurs that in African countries relevant and proper records management laws existing are not enforced for proper records management. Giving an example of e-records the author concludes that it is useless to manage these records without procedural and legal laws, since they are not fully recognised in law courts as legal evidence because of their propensity for alteration at whims. In contrast, Kenya has put in place legislation and regulations that should guide e-records management practices. The regulatory framework includes:

The Public Archives and Documentation Service Act, Cap 19: it is the principal law that governs management, preservation, and disposal of public records. The act mandates the director of the Kenya National and documentation service (KNADS) among other functions to: examine any public records and advice on their care preservation custody and control, require transfer to the custody of the KNA and documentation service; public records he/ she considers should be housed in the national archives and authorise the destruction of public records judged to be of no further administrative or reference value to creating office. Section 5A of Cap 19 states that every permanent secretary or head of government department or chief executive of a state corporation or local authority shall supply to the director two copies of any published or generally documented documents or reports produced by the office, whether in hard copy or microfilm and the creating office may prescribe the period for which the document shall remain restricted from circulation to the public offices or the members of the public. Besides, section 8 of the public archives and documentation service Act, Cap 19, indicates that it is an offense to destroy public records without the directors of KNADS authority.

Ministry of state for public service (DPM) circular on personnel records-ref.No.DPM.12/6AVol. (71) Of 12th March 2008: The circular (personnel general letter), number 1/2008 of the 12 March 2008, provides guidelines on the retention of various categories of personnel records in the public service. The prescribed retentions periods should be applicable for personnel files for officers in similar job groups in the local authorities, the judiciary and states corporations. The circular further advises that any deliberate destruction must be communicated to the director of KNADS for guidance.

Government financial regulations and procedures, Chapter 23, sections 4:2-5: this regulations and procedures are provided to guide the management and disposal of account documents. The regulations elaborate that an accounting officer may permit the destruction of accounting books and documents provided such records have been audited and have no archival value. Accounting documents with outstanding audit queries should not be destroyed. The director of Kenya national Archives may be requested to examine the records before their destruction.

The Records Disposal Act, Cap 14, 1962 (Revised 2009): the act facilitates the management and disposal of court records in Kenyan courts. It mandates the Chief Justice and the registrar of the high court, in consultation with the director of the KNADS to make rules for the disposal of court records. The statutes establish the authorities and procedures for disposing of records covered under the act. The act also defines the offices under the office of the Attorney-general and provides a records retention schedule of the records covered in the act as well as the procedures for the disposal.

Public Procurement and Disposal Act, Cap 412C, 2005: The act requires procuring entities to manage procurement records properly and effectively. Records must be recognised as a critical resource for proper management. The authority is mandated to issue circulars and guidelines on the content of the procurement documentation, and regulations 34 (2), which states that the authority may issue guidelines about the use of records management, filing, and storage of procurement documents. The act further empowers the director general of the public oversight authority (PPOA) to inspect the records and accounts of a procuring entity.

3.2.2.1 E-records standards and best practices

Standards and best practices are prepared internationally by the international organisation for standardisation (ISO) which is a worldwide federation of national standards bodies (ISO member bodies). Consequently, there are a number of standards that guide the management of records which include: ISO 15489-1 information and documentation, ISO/TR 15489-2 Records management, ISO 900:2015, ISO 23081- managing metadata, ISO/TR 15801:2005 Electronic imaging in addition to strategic plans and codes of conduct and ethics among others. Besides, the ISO standards, there are other standards developed in the management of e-records including DoD 5015-2 US Department of Defense: Design criteria standards for electronic records management applications, British standard BS 1008:2008, Evidential weight and legal admissibility of electronic information specification. The Parkerian Hexad Model advocates for organisations investing in better policy writing and enforcement, procedures and methods, implementation of the policies and improving the available technology infrastructure.

The ISO 9001:2015 to which many organisations and institutions worldwide including Moi University are compliant to, clause 4.2 document requirements, stipulate that the quality manual system documentation shall include among others, documents including records, determined by the organisation to be necessary to ensure the effective planning, operation and control of process.

Furthermore, clause 4.2.4 on control of records asserts that records established to provide evidence of conformity to requirements and of the effective operation of the quality management system shall be controlled and that the organisations shall establish a documented procedure to define the controls needed for the identification, storage, protection, retrieval, retention and disposal of records.

In Kenya, the local standardisation body Kenya Bureau of Standards (KEBS), has put in place a number of progressive standards in support of e-records management from the early 2000s. Between the years 2010 and 2013 specific e-records management standards have been developed and adopted by KEBS. They include KS 2229:2010-Electronic records management systems-functional requirements; KS ISO/TS 21547:201 Health informatics-security requirements for archiving electronic health records-guidelines, KS2374:2012-Electronic records management systems-implementation guide, KS2391:2013-electronic signatures-metadata requirements, (Kenya Bureau of Standards 2014). However, the adoption and implementation of standards in Kenya institutions is very low.

3.3 Security classification of e-records process handling to facilitate description, control disposal, and access

This study among other objectives sought to investigate the security classification of e-records process handling to facilitate description, control disposal, and access. To understand the basis of security classification of e-records process handling to facilitate description, control disposal, and access,

3.3.1 Practices and initiatives in e-records security management

With more complex technologies being developed in the e-records lifecycle process, there is greater need for standardised procedures to apply in order to achieve security of e-records. In recent years so much has changed on how activities are carried out including medical (Electronic health records management), e-governance, ability to file taxes online, cloud storage and the evolution of security threats which have led to complexity in e-records management. Consequently, at any time organisations develop new methods of creating, maintaining, storing, preserving and disposing of e-records. Such innovations should inevitably be accompanied by methods of harnessing the new technologies and protecting the e-records (Bey 2012; IRMT 2011; Russell and

Gangemi 2006). Parkerian model highlights that, the complexity of e-records security which has resulted from the advancement in technology, calls for a more robust, comprehensive and complete intellectual model to address e-records security issues (Cukier 2010, Bhaiji 2008; Parker 2002). UNAIDS (2016), defines security as a collection of technical approaches that address issues covering physical, electronic, and procedural protection of e-records collected. ISO 15816 (2002) on the other hand explains that security management aims to ensure that assets, including information, are protected appropriately and cost-effectively. For instance, in order to protect proprietary interests and intellectual property, organisations need to control the handling of their information in all forms during its storage, processing, and transmission between and within an organisation over both private and public networks. According to the Charles Darwin University (2017), the security of University records ensures proper practice of creating, storing, using and making records available securely with due regard to permitting access for those members of the University community with a genuine need to know the information contained within the records and who have the proper authority to access them. In the researchers' view, it is a process that must begin before and/ after e-records creation to disposal cycle, thus, enhancing e-records security. Although, in theory, the issues of security seem to be separated, in practice the activities should be worked on seamlessly and simultaneously throughout all e-records management process.

3.3.2 Security classification of e-records

Classification is a systematic identification and organisation of e-records into categories conferring to logically structured conversations, methods and procedural rules in a system as represented in a classification scheme (Bantin n.d., ISO 2001). Benett (2011) adds that the classification of e-records is a shorthand way of determining how this information is to be handled and protected. ISO (2001) explains that classification is a powerful tool that helps organisation work effectively by ensuring records are named in a consistent manner over time, assisting in the retrieval of all records relating to a particular function or activity, determining security protection and access appropriate for sets of e-records, allocating user permissions of access to or action on particular groups of records, distributing responsibility for management of particular sets of records, distributing records for action and determining appropriate retention periods and disposal actions for records. It should take account of business needs, for example, unauthorised access or damage to the information therein.

However, to understand e-record classification, analysis of business process should be carried out. Analysis of business process involves gaining an understanding of what an organisation does and how it does it and also gaining an understanding of the existing systems available. The analysis provides an understanding of the relationship between the organisation's business and its records (Glavan and Vesna 2017; ISO 2001). AIIM (2008) asserts that far too many good records management programmes are suffering from lack of user acceptance and one way of solving the puzzle is by developing a programme that is tightly coupled with the underlying business process. For the reason that business process are the organisation's strategic assets, analysing the processes yields a documentation describing the organisation's business process, a business classification scheme that shows the organisation's activities and transactions in hierarchical relationship and a map of the organisation's business process that shows the points at which e-records are created or received as products of the business function (ICA 2008; DIRKS manual 2003; ISO 2001). These sentiments are shared by ISO (2001) that for organisations to conform to sound e-records management, they have to design a records management system that prescribes the development of a records classification system based on the analysis of business activities. This is because organisations have the responsibility to create, use and retain records in support of their business functions, thus, making it logical to organise, maintain, store and dispose of the e-records in accordance with the same functions that call for a proper functional classification system that meet the needs of the organisation (Tasmania Archive Heritage Office (TAHO) 2015; ISO 2001).

Moreover, e-records security classification designates the sensitivity of e-records that governments, organisations, and institutions have created, and stored in the conduct of their business functions including those received from external sources. It comprises a set of instructions, procedures or sources that identify and protects a system, a plan, program and e-records including the reasons for classification (for example, whose disclosure could have adverse consequences to the organisation) (Centre for Development of Security Excellence 2017; University of Tasmania 2014; Bey 2012; Parker 2002).

Moreover, every organisation has diverse e-records including, but not limited to, sensitive records that can only be accessed by certain personnel and those that can be accessed by everyone. For instance, in government, e-records are classified not just by assigning value to the e-records, but also as means to secure them. This gives the measure by which organisation assigns a level of sensitivity and an owner to each piece of e-records that he/she creates, receives and maintains (Public Service of Kenya 2010; Mishra 2011). Various factors influence the e-record security classification. They include, but are not limited to the value, the nature of the organisation, and age of the record. Mishra (2011) in a study of information security and cyber laws in New Delhi, India outlined considerations in classification of a record. These considerations include; how much value that information has to the organisation, how old the information is, and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

Around the world, classification is identified as an essential factor in protecting e-records. For example, in the USA the Department of Defence (DoD) developed a manual DoD 5200.2 to guide the development of security classification that includes access controls, declassification and downgrading (DoD 2002). In 2003, National Archives of Australia prepared an overview guide on classification tools that could assist commonwealth countries to support records management process. Furthermore, the State Records Authority of New South Wales and the National Archives of Australia, and ISO have developed guidelines that can be applied globally in e-records security classification among others.

E-records security classification may be ascribed as public, sensitive, top secret, secret, confidential, classified, unclassified, and restricted (Mishra 2011; Collette and Gentile 2006; DoD 2002). Kahanwal and Singh (2013) state that the value of a record springs from the ways it is interpreted and applied in an organisation, for instance, *restricted* (may be applied to personnel social security number, drivers licenses, financial account numbers, health records); *internal information* (it is the information category, which is accessible only with the reason to know, for example, unpublished research, notice of meetings, seminars, training, advertisement) and public information (the information is related to both the staff and the public for instance game schedules, medical camp schedules, and examination schedules. Public Service of Kenya (2010) asserts that government of Kenya gives security classification and levels of access to classified information as follows: top secret (information and material, whose unauthorised disclosure would cause exceptionally, grave damage to the Republic), secret (information and material whose unauthorised disclosure would cause serious injury to the interests of the Republic), confidential (information and material whose unauthorised disclosure would be prejudicial to the interests of the Republic), restricted (information and material whose unauthorised disclosure would be undesirable in the interests of the Republic).

3.3.3 Access control

Access is the right, opportunity, means of finding, using or retrieving modifying among others of e-records**.** Thus, access control is the means to ensure that access to e-records and the system that holds them is authorised and restricted based on the business and security functions (ISO/IEC 2014; ISO 2001). This implies that e-records management system should provide reliability of complete, organised, accessible and secure records, secure integrity by authority control systems, compliance with legislative, regulative and appropriate, business requirements, reflected comprehensive range of appropriate business activities and systematic creation. In this regard, institutions such as Moi University must be able to control access to e-records and in which circumstances they can be accessed because the records may contain personal, commercial or operationally sensitive information (ISO 2001).

Access control is an individual security control that is applied to individual e-record, which restricts or denies control on a range of properties such as authorise view document, view metadata, update a document, sharing, update, rectify, modify, and delete. The access control is used to secure e-records and other university assets such as ICT infrastructure, finances employees and students among others (TAHO 2015; Yorkland Controls 2007). Bandar and Colin (2007) in their study on access control requirements for processing electronic health records in Australia emphasised that an access control mechanism should be applied to limit the actions or operations that a legitimate user of a computer system can perform.

Bigirimana, Jagero and Chizema (2015) in their study of an assessment of the effectiveness of e-records management at the African University, Mutare, Zimbabwe found that an effective e-records management system is critical in ensuring that movement and location of records are controlled in a way that any record can be accessed when needed and that there is an auditable trail of recordable transactions. They further stated that the record-keeping system whether paper or electronic should include a set of rules for referencing, titling, indexing and if appropriate security marking of records. These should be easily understood and should enable the efficient retrieval of information. They further stated that confidentiality and accessibility should concurrently be adhered to through proper classification, labeling, indexing, and file naming.

Therefore, the issues of access rights and restriction to e-records, how and when e-records are stored, security of e-records, transfer, analysis rights, and access policies is a matter of concern to an organisation (Omotosho and Emuoyibofarhe 2014; DoD 2001; ISO 2001). ISO (2001) reiterates that organisation should identify the transaction or business activity that the record documents, identify the business unit to which the records belong, check the access and security and the security classification to establish whether the activity and the business area are identified as areas of risk or have security consideration and/or are legally required restrictions, allocate the appropriate control mechanisms for handling, and record the access or security status of the record in the record system to signal the need for additional control measures. Hence, assigning rights and permissions to roles with user accounts then associating to a role among others, must be done appropriately and consultatively including the creation and management of the system access accounts for authorised users. Furthermore, appropriate security and access should be determined by analysis and appraisal of the records series and business rules developed for the acceptable management of these records (TAHO 2015; Dr. Stevens's Hospital Access Control Policy 2003). For this reason, role-based access control where an individual who needs to access information and where each role defines the set of privileges and operations an individual can perform should be considered as a means of ameliorating most of the security-related issues (Omotosho and Emuoyibofarhe 2014).

The Kenya access to information act no. 31 of 2016, provides a framework for public entities (such as Moi University) and private bodies to proactively disclose information that they hold and provide information on request in line with the constitutional principles, as well as a framework to facilitate access to information held by private bodies in compliance with any right protected by the constitution and any other law. Furthermore, they should promote routine and systematic information disclosure by public entities and private bodies on constitutional principles relating to accountability, transparency and public participation and access to information. They must provide for a person who may disclose information of public interest in good faith and a framework to facilitate public education on the right of access to information under the act.

There is need to provide limited access using a scheme of security categories or classification and security clearances where users can then be allocated one or more security clearances which prevent access to all classes of file records at higher security classification. Moreover, there is the need to ensuring access to e-records, systems networks and applications by authorised users, the accuracy of e-records is secured, and that e-records are only accessed by authorised individuals. A variety of methods including physical security, password protection, intrusion detection and prevention, security classification labeling, encryption, security shredding, and e-records security awareness can be used to secure e-records assets (TAHO 2015). ISO (2001) advices that, access to records is restricted only where it is expressly required by business need or by law. The access and security classifications may be assigned in consultation with the business unit to which the records belong. Restrictions may be imposed for a stated period to ensure that the additional monitoring and control mechanisms required for these records are not enforced for an extended period.

3.4 Security threats on e-records

The third objective of the study was to investigate security threats on e-records. To understand the threats, the researcher reviewed the literature on threat assessment, existing and potential e-records threats, policies and regulatory frameworks, and cyberspace security threats.

3.4.1 Threat assessment

E-records effort should be oriented towards threats specific to the organisation and other related government entities. An organisation should conduct threat assessment with specific priority system with the intention of creating a threat- base understanding of the priorities. Similarly, the organisation needs to be continuously reviewed to determine the likelihood of cybersecurity events. Perhaps, based on the knowledge gained from the assessment, the organisation is able to identify potential threats that may affect the organisation (Canada Investment Industry regulatory organization (IIROC 2015).

US Department of Commerce, National Institute of Standards and Technology (NIST) explains that threat assessment is used to identify, estimate and prioritise threats to organisations operations (including missions, functions, image, and reputations to mention a few). The purpose is to inform decision-makers about relevant threats to the organisation, threats directed through organisations against others, vulnerabilities both internal and external to the organisation, the impact (harm) to the organisation that may occur given the potential for threats exploiting vulnerabilities, and the likelihood that harm will occur. Thus, the result is a determination of a threat or threats.

While security risk assessment provides the means to identify and address potential threat factors, failure to perform assessment effectively can lead to missed opportunities, both to avoid and capitalise on threat events (City University of Hong Kong 2016)

3.4.2 An overview of existing and potential threats on e-records

The proliferation of increasingly complex, sophisticated technologies has led organisations to experience threats in e-records security daily from employees, competitors through criminal and corporate spies to governments and external environment to mention a few (Calder 2013). These sentiments are shared by Parkerian Model that with the advancement of sophisticated technologies and the trend at which new trends are evolving, threats are inevitable (Bey 2012; Andress 2011; Parker 2002). E-records security threats have been in existence as early as 1990's as evidenced by studies carried out in developed countries, which raised numerous threats concerns in e-records management (Duranti and MacNeil 1996; Cox 1994; Cook and Frost 1993; Cook 1991; United States National Historical Records and Publications Commission 1991). The same concerns have been raised in developing countries **(**Tough 2000; Enwere 1997**;** Nyirenda 1994). As technology advances, several security threats have emerged causing widespread damage to national security, economic growth, and critical infrastructures. Mutula (2013) noted that in Africa though countries such as Mauritius, Egypt and Seychelles have made significant progress in developing ICT infrastructures, they still lag well behind global leaders such as Canada, Korea, and the US in developing e-records security infrastructure.

IRMT (2009) assert that the ICT infrastructure does not solve the problem of managing e-records security management. However, availability of ICT is the primary underlying factor for managing e-records. Asogwa (2012) observes that, while technology has brought enormous benefits to organisations, it has simultaneously introduced a number of challenges and difficulties including the risks of losing data and records, risks to reliability and authenticity of e-records, loss of security and privacy, increased costs of managing records and decentralisation and increased need for information technology specialists.

California e-records handbook (2012) explains that e-records keeping systems are more vulnerable to undetected alteration, loss or unauthorised disclosure of information that is in hard copy or microform system. Research has shown that insider threats such as authorised personnel, friends, and co-workers are more challenging to address than external threats (Omotosho and Emuoyibofarhe 2014). Insider threats (employees or trusted third parties) can intentionally or unknowingly damage a system and steal information including social security numbers for personnel, gain or destroy or delete critical records of the organisation or personnel. This is because they enjoy exclusive access to an institutions e-records and systems, and are thus, uniquely positioned to inflict significant damage. Similarly, vulnerability is created to e-records and systems when all staff (through unauthorised sharing of access privileges) can access vital information of the organisations' operation (Canada Investment Industry regulatory organisation (IIROC) 2015; UN NACCHO 2015). These sentiments are shared by Africa cybersecurity reports (2016) that insiders are bigger security threats compared to outsiders for African organisations. The insider threats include fraud involving information or employee abuse of information technology systems and information. The Parkerian model also identifies personnel as a significant threat to e-records and systems (Parker 2002).

This is exacerbated by the fact that e-records are more vulnerable to undetected alteration, unauthorised disclosure of information, improper or careless handling, accidental erasure or mislabeling of storage devices and physical damage to hardware and software **(**Raaen 2017; Greizter 2014; Ernest and Young 2013; Bey 2012; Dean 2012; Parker 2002; Parker 1998). Ngoepe et al. (2010) in their study on security, privacy and ethics in electronic records management in the South African public sector, identified some security issues in ERM. They identified illegal access and use of records, data alteration, and destruction. In the same breath Bennett (2011) in his study of security in records management in the United Kingdom, noted that e-records are particularly vulnerable to unauthorised or inadvertent change and loss. In the last two decades, many authors have expressed concern about the state of e-records in developing countries saying they do not meet international best practices, and this has impeded the move towards openness in the region. Moreover, where inaccurate e-records are used for development planning or holding governments and organisations accountable, the evidence base required to formulate policy, manage state functions, build reliable systems and monitor official transactions is undermined (Wamukoya 2013; IRMT 2012; Thurston 2012; Asogwa 2012). Kemoni (2009) in his study, on the management of electronic records: a review of empirical studies from the Eastern, Southern Africa Regional Branch of the International Council on Archives (ESARBICA) region, noted that apart from South Africa, most countries in the ESARBICA region face various problems in managing electronic records. Another study by the United States General Accounting Office (2003), on the e-records management and preservation, found that complex e-records are being created in volumes that make them difficult to organise and keep accessible. These problems are attributed to computer hardware, application software and even storage media obsolescence which may leave behind e-records that can no longer be read. As a result, valuable government information may be lost. Asogwa (2012) similarly found the challenges of managing e-records in developing countries that included weak legislative and organisational infrastructures, inadequate ICT skills and competencies, security and privacy problems, corruption and inadequate funding, political instability, continually changing technology, deterioration of digital media, problem of reliability and authenticity of records, legislative constraints and more.

3.4.3 Inadequate or lack of policies and regulatory frameworks

The other significant threats to e-records security management are inadequate or lack of policies and regulation (Asogwa 2012; Marutha 2012; IRMT 2011; Moloi 2009; Mnjama and Wamukoya 2007; Moloi and Mutula 2007; Makhura and Ngulube 2005; Wamukoya and Mutula 2005). Looking at the developed countries scenario, the Republic of Korea, Netherlands, UK, and Denmark to mention a few, have sound policies for computer matching and privacy protection, computer security, electronic management, records security, electronic freedom of information among others (Mutula 2013; Relyea 2002). Asogwa (2012) bemoans the many gaps in legislative prescript as a result of the fast advancement of technology. ISO (2001) asserts that a policy framework helps among others to fight cybercrime, controlling access to information, planning of business continuity, complying with legal and policy requirements, developing and maintaining in-house software, controlling e-transaction security, detecting and responding to information security incidents. Unfortunately, despite policies and regulations being vital to organisations in e-records security management, most developing countries lack e-records management policy as indicated in section 3.2.2 (Maseh 2015; Lappin 2013; Williams 2013; Asogwa 2012; Nengomasha; 2009; Moloi and Mutula 2007; Sejane 2005).

A study carried out by IRMT (2011) on the alignment of records management with ICT in East Africa showed that some governments in the region including Kenya had policies in place for managing records, but in practice they did not address e-records, and there was no evidence that records management practices had been applied to e-records. Keakopa (2007) appreciates that South Africa has a well-developed statutory and regulatory policy framework to guide public service agencies to manage e-records. However, the limited number of government departments have taken advantage of these available overarching policy guidelines by customising internal mechanisms for e-records management. Hardware and software failure are also a significant threat to e-records security management. Records in e-formats are hardware and software dependent, and whenever there is the hardware failure, this affects the e-records. The increased use of e-records to support business functions requires attention to the hardware and software maintenance to avoid disruptions that are of temporary and catastrophic nature (Raaen 2017).

Furthermore, migrating e-records to new hardware and software platforms must be undertaken meticulously to enable them to remain accessible and authentic. Unlike paper records which can be moved, filed and otherwise used and reused without change, e-records need to be managed and preserved to secure their authenticity as evidence. The records can only be read and understood if the existing hardware can read the storage medium and if the programmes used to create the e-records are still available. Moreover, the movement of e-records from older to newer hardware and software (migration) also creates a security threat to e-records over time, and this requires careful planning (Raaen 2017). Mnjama and Wamukoya (2007) observe that crucial resources such as equipment, basic supplies, and finances are not often made available in a majority of government environment in developing countries including, Kenya. They observed that with a few or non-existent trained and qualified personnel in records management and the low status accorded to records work, the principles and standards that should guide records and information work were never included as part of the organisation strategic plan.

3.4.4 Impact of cyberspace

Cyberspace is the digital environment made up of digitised records that are used and shared, through networks and/or including the physical systems, such as computers and databases that enable exchange of information as well as the users who make use of the system (US national association of county and city health offices (NACCHO) 2015; Friedman and Singer 2014).

Therefore, the broader reach and impact of cyberspace which is accelerating across national and international boundaries is making it a complex challenge for any government to address issues of e-records security (Ministry of ICT, Kenya 2014; Omotosho and Emuoyibofarhe 2014). Wamukoya and Mutula (2005) state that inadequate security and confidentiality controls are significant factors contributing to the failure of capturing and preservation of electronic records in Eastern and Southern African educational institutions. Similarly, Myler and Broadbent (2006) posit that information security issues such as cybercrime, privacy, virus attack, and commercial data mining are the major concern to academic institutions. Cybercrime is a term used to describe ICT attacks including viruses. According to the government of Kenya, cyber-attacks are continuously evolving to a great extent faster than cyber defenses (Ministry of ICT, Kenya 2014). The Ministry of ICT in Kenya (2014) provided a cyber-attack snapshot of sophistication trend from 1980-2014 in Kenya, East Africa and internationally that is presented in figure 7

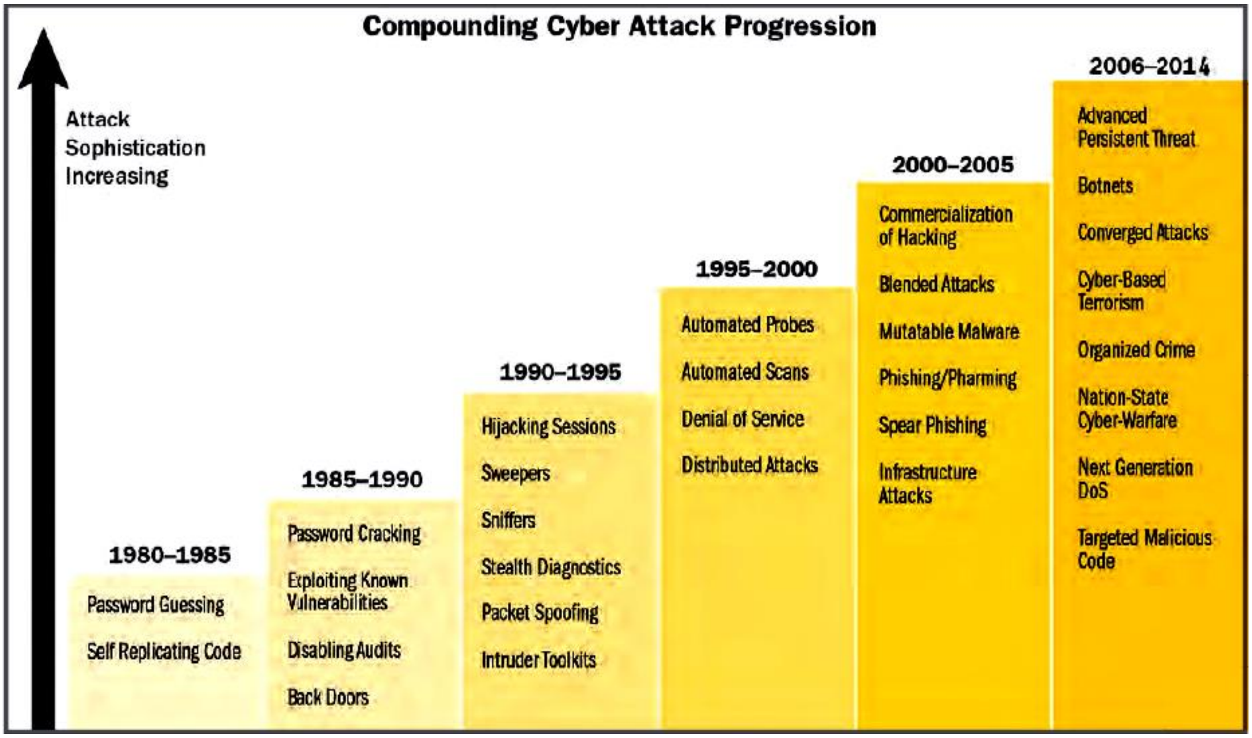


Figure 7: Trends in Cybersecurity of cyber-attacks from 1980-2014 (Source: Ministry of ICT National Cyber-Security Strategy Report 2014)

Kenya cybersecurity report (2015) observes that cybercriminals have advanced to such a degree that it is almost impossible to detect intrusions without the use of advanced continuous monitoring and detection methods. The hacktivists and crackers manipulate the ICT infrastructure which compromises security leading to corruption or loss of information, misuse or theft of information, identity theft and unauthorised use of client information, they alter, disrupt or destroy sensitive personnel business and government information. Omotosho and Emuoyibofarhe (2014) noted that in an age of identity theft and data snooping, the health care industry has become one of the most sought-after domain by cyber attackers because the transition from paper-based health systems to electronic health records systems has given data thieves compelling reasons to attempt cracking hospital networks due to the value of medical data it contains. Also, viruses (computer programs written by devious programmers and designed to replicate themselves and infect computers and other storage devices by copying themselves into a file and other executable programmes when triggered by the specific event are a security threat to e-records (Khan et al. 2017). Transmission of computer viruses that can affect third parties and lead to potential liability, services interruptions and security breaches that compromise e-records security management are of great concern to organisations including Moi University (Waithaka 2016; Kenya Cyber Security Report 2015). Lack of antivirus software to scan the computer for malware may lead to loss of e-records (UN NACCHO 2015; Microsoft 2013).

The cybercriminals went a notch high with the introduction of a ransomware virus which encrypts data on infected computers and demands a ransom payment to allow users access worldwide. For instance, between January 2015 and April 2016, the USA was the region most affected by ransomware, with 28% of global infections. Canada, Australia, India, Japan, Italy the UK, Germany, the Netherlands, and Malaysia being among the top 10. The report further indicates that 43% of ransomware victims were employees in organisations (Symantec special report 2016). In 2017, a day described by Yokahama (2018) ‘The day the world cried’ in his publication on business management and cybersecurity, digital resiliency for executives, WannaCry virus attack hit 150 countries where more than 200, 000 computers were infected in less than three days (Microsoft 2017; Yokahama 2018). According to the England National Audit office (2017) on Friday of 12th May 2017, WannaCry which encrypts data on infected computers and demands a ransom payment was released worldwide. WannaCry was the most significant cyberattack to affect the National Health Service in England. Luckily, a significant part of Africa was spared. However, some countries on the African continent were affected, including South Africa, Nigeria, Angola, Egypt, Mozambique, Tanzania, Niger, Morocco, and Tunisia (Kaspersky lab report 2017).

Although Kenya was not among countries affected by the WannaCry attack, it lost USD 21 million to cyber-attacks in 2017 alone, while in 2015 and 2016 Kenya lost, USD 150 and USD 175 million respectively (Kenya cybersecurity report 2016). According to a 2016 Kenya cybersecurity survey, there is an increased rate of cybercrime in Kenya. Most of the respondents (70.6%) experienced cybercrime in one way or another; out of these, 34% was through work, while 66% at personal level. Furthermore, network security threats are spread over the internet and are witnessed frequently, while their management is less advanced (Raaen 2017; Kenya Cyber Security Report 2015; Ministry of ICT, Kenya 2014; Mishra 2011; Yeh and Chang 2007). Lack of intrusion protection and detection to monitor network or system activities for malicious and unauthorised activities results to network security threats. These threats may include, but are not limited to, social engineering (obtaining confidential network security information through nontechnical means such as posing as a technical support person and asking for peoples passwords); Trojan horse programs (delivery vehicles for destructive code, which appear to be harmless or useful software programs such as games); access attacks (which exploits network vulnerabilities in order to gain entry to e-mail, databases or the corporate network); denial-of-service attacks (which prevent access to part or all of a computer system) unauthorised access.

3.5 Measures to protect unauthorised access to e-records

E-records system should routinely capture all records within the scope of the business activities it covers, organise the records in a way that reflects the business activities it covers; protect the records from unauthorised alteration or disposal; routinely function as the primary source of information about actions that are documented in the records; and provide ready access to all relevant records and related metadata (ISO 2001). Organisations' e-records such as sensitive information on their employees, salary information, financial results, business plans, trade secrets, research and other information that gives a competitive edge, require limitations to access them for the reasons of confidentiality, proprietary nature of the information or due to legal protection (ISO 2001; Kahanwal and Singh 2013). Access management processes and technologies are not well adapted in most organisations leading to unauthorised and inappropriate access to highly sensitive e-records (Kabeberi 2015). According to the Moi University ICT policy (2011) gaining access to the university's information technology resources does not imply the right to use those resources. Furthermore, it states that the university reserves the right to limit, restrict, remove, or extend access or privileges to material posted to its information technology recourses, consistent with the policy, applicable law or as the result of university disciplinary processes and irrespective of the originating access point. Asogwa (2013) corroborates this point that only authorised persons should have access to e-records, thus preventing information from being stolen or damaged. This practice ensures the protection of privacy and confidentiality and prevents inappropriate disclosure of information that could harm the organisation or infringe the privacy rights of individuals if records are not adequately managed.

Organisations are increasingly choosing not only to create records electronically, but also to store, retrieve and use them in computerised form for long periods (IRMT 1999). As presented in the review of literature in section 3.5 and 3.5.1 controls; therefore, must be applied from the outset if the e-records are to be secured as reliable sources of information over time. Moreover, because the control of e-records is dependent upon technology, records professionals must become more aware of how different technologies work and how they affect records and record-keeping.

When management chooses to put up measures of e-records security they do so by implementing one or more types of controls. For instance, they may use administrative or procedural controls, which consists of approved written policies, procedures, standards and guidelines (Mishra 2011; ISO 2001). ISO (2001) explains that the objective of the policy should be the creation and management of authentic reliable and usable records, capable of supporting business functions and activities for as long as they are required. These procedural controls form the frameworks for running the business and managing people. They inform people on how the business is to be run and how the day to day operations are to be conducted and the policies should be communicated and implemented at all levels. Policy development has been emphasised by many scholars as key to good e-records management for they clearly set out the organisations expectations regarding individuals' roles and responsibilities, ownership, access control, security classification among others (Ambira 2016; Maseh 2015; Bigirimana et al. 2015; Asogwa 2013; Erima 2013; Kyobe et al. 2009; Kemoni and Ngulube 2008; Wamukoya and Mutula 2005).

Mishra (2011) and ISO (2001) further explain that laws and regulations created by government bodies are also a type of administrative control because they inform the organisation. They include, for example, Kenya's records management procedures manual for the public service (2010), the constitution and cybercrime bill which provides guidelines on e-records security management. The administrative controls may also include university security policy, ICT policy, password policy, hiring policy and disciplinary policies. Logical controls or technical controls are also measures used to protect unauthorised access (Mishra 2011, ISO 2013). The logical controls may include the use of software and data to monitor and control access to information and computing systems. This may include, passwords, antiviruses, network, and host-based firewalls, network intrusion detection systems, access control lists and data encryption and principle of least privilege.

Besides, physical control is a measure that is also used to protect unauthorised access to e-records. Such physical controls help monitor and control the environment of the workplace and computing facilities. They also monitor and control access to and from such facilities. The physical controls may include doors, locks, heating and air conditioning, smoke and fire alarms, fire suppression systems, cameras, barricades, fencing, security guards, cable locks and separation of duties. Security and records professionals need to focus on establishing security situational awareness within their respective organisations that is, the regular, repeatable development and communication of the organisation knowledge of its people, ICT infrastructure, threats, incidents and vulnerabilities (Kenya Cyber Security Report 2015). The Kenya Computer and Cybercrime Bill (2017) warns that a person who causes whether temporarily or permanently a computer system to perform a function by infringing security measures with intent to gain access and knowing such access is unauthorised, commits an offence and is liable on conviction, to a fine not exceeding five million Kenya shillings or imprisonment for a term not exceeding three years, or both.

3.5.1 Measures to protect intranet against external and internal cyber-attacks

The Internet is a mechanism for information dissemination and medium of collaboration and interaction between individuals and their computers without regard to geographical location. It symbolises a critical underlying technical idea, that of open architecture networking where the choice of any individual network technology was not dictated by a particular network architecture, but instead could be selected freely by a provider and made to interwork with the other networks through a meta-level internetworking architecture. Consequently, in open architecture networking, an individual network may be separately designed and developed, and each may have its unique interface, which it may offer to users and other providers including other internet providers.

Similarly, each network can be designed in accordance with a specific environment and user requirement of that network (Misha 2011; Leiner et al. 1997).

Most organisation especially institutions use extranet and intranet, which are both private. Extranet is a private network that uses internet protocols (IP), network connectivity and possibly the public communication system to securely share part of an organisations e-records and other information or operations with suppliers, partners, customers or other business (it is extended to users outside the company), while intranet which is of interest to this study, is a private network that uses IP, network connectivity and perhaps the public telecommunication system to securely share part of an organisation's e-records and other information or operations with its employees. In addition, it acts as a core management tool that streamlines practices and provides a means of resource and knowledge sharing, visibility and marketing, management and also acts as a daily messaging channel to help drive the business effectively among employees, departments, and units worldwide (Marja 2011; Gupta 2007; Cutlip et al. 2006).

Intranets are designed to permit users who have access privileges to access the intranet of an organisation. Within an intranet, web-servers are installed in the network browsers technology to be used as the common front end to access information on servers such as financial, graphical, or text-based data (Daya 2014). Perhaps being private and only accessed by authorised users will give the impression that the intranet is secure. However, that is not the case as it requires sophisticated cybersecurity measures to protect it against external and internal cyber-attacks. Cybersecurity are the measures put in place to protect e-records and other assets from compromise, theft or loss by a determined external attacker or an insider threat within the organisation (Australian government 2017). The measures may include, but are not limited to:

Establish role-based access controls and implement system logging: role-based access control grants or denies access to network resources based on job functions. This limits the ability to individual users, or attackers to reach files or parts of the system they should not access. Therefore, the permissions based on the level of each job function needs to perform its duties and work with human resources to implement standard operating procedures to remove network access of former employees and contractors. Besides, limiting employee permissions through role-based access controls can facilitate tracking network intrusions or suspicious activities during an audit (NIST computer security information center 2018; WaterISAC 2016; Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) 2013).

Use only strong passwords, change default passwords and consider other access controls: Use strong passwords to keep your systems and information secure, and have different passwords for different accounts. Passwords should have at least eight characters because longer passwords are stronger. Including uppercase and lower letters, numerals and special characters will strengthen passwords too. United States Computer Emergency Readiness Team (US-CERT security tips (ST04-002) 2018; US-CERT security tips (ST05-012) 2018; Microsoft 2017; WaterISAC 2016).

Develop and enforce policies on mobile devices: The proliferation of laptops, tablets smartphones and other mobile devices in the workplace presents significant e-records security challenges. The mobile nature of these devices means they are potentially exposed to external, compromised applications and networks and malicious actors. Furthermore, contributing to this challenge is the increasing trend of organisations allowing employees to use their personal electronic devices for work purposes, known as the "bring your own device (BYOD) phenomenon (United States Computer Emergency Readiness Team (US-CERT) 2017; Microsoft 2017; US Department of Commerce, National Institute of Standards and Technology (NIST) 2016; WaterISAC 2016; US Department of Commerce, National Institute of Standards and Technology (NIST) 2013).

Maintaining an accurate inventory of control systems devices and eliminate any exposure of the equipment to external users: this involves prohibiting a foreign machine to discourse directly to a machine on the organisations' network on the internet. A thorough assessment of the system should be conducted frequently (WaterISAC 2016; Glantz and Landine 2012; Gupta 2007).

Implement network segmentation and apply firewalls by classifying and categorising ICT assets, the e-records, and personnel into groups and then restricting access to these groups: Access to network areas can be restricted by isolating them entirely from one another. Creating network boundaries and segments empowers an organisation to enforce both detective and proactive controls within its infrastructure (WaterISAC 2016; Kumar and Malhotra 2015).

Use secure remote access methods: The ability to remotely connect to a network can add a great deal of convenience for the end user. Though a secure access method such as a virtual private network (VPN) should be used if remote access is required (WaterISAC 2016; Microsoft 2009).

Other measures may include, but are not limited to, issuance and use of digital certificates or similar means of authentication, encryption of messages, inventory authorised and unauthorised devices, inventory of authorised and unauthorised software, secure configurations for hardware and software on laptops, workstations and servers (WaterISAC 2016; Kumar and Malhotra 2015; Glantz and Landine 2012; Gupta 2007).

3.6 E-records confidentiality, integrity, availability, authenticity, possession/control and utility

The second objective of the study was to establish how e-records confidentiality, integrity, availability, authenticity, possession or control and utility are achieved. The intention was to establish e-records security ethical values and understand the vetting process what the process entails.

E-records confidentiality: Confidentiality refers to the property that e-records is not made available or disclosed to unauthorised individuals, entities, or processes or preventing the disclosure of information to unauthorised individuals or systems (Northeastern University policy 2018; Bristol clinical commissioning group records management policy 2016; Steichen 2012; Parker 2002). It relates to the right to protect e-records and the systems that hold them during storage, transfer, and use in order to prevent unauthorised disclosure (UNAIDS 2016). Mishra (2011) explains that breaches of confidentiality take many forms, for instance, permitting someone to look over your shoulder at your computer screen, while you have confidential information displayed on it could be a breach of confidentiality, if a computer containing sensitive information about the university's employees is stolen or sold, it can result in breach of confidentiality. This thinking is supported by the Parkerian Hexad Model, which asserts that confidentiality is the limited observation and disclosure of knowledge. The e-records that are confidential in nature may include identifiable student and parent e-records, contracts, research records, alumni and donor records, personnel records, university financial records, computer passwords, university proprietary information and other e-records authorised by laws and regulations, international privacy regulations and available policies, procedures and guidelines (Northwestern University records policy, 2018). Personnel responsible for ensuring the confidentiality and appropriate use of institutional e-records to which they are given access, ensuring the security of the equipment where such e-record is held or displayed, ensuring the security of any accounts issued in their name and abiding by related security rights of students and staff concerning the use and release of personal information as required by law or existing policies must be vigilant to enhance confidentiality of e-records (Moi university ICT policy 2011; MoReq 2001). According to Bigirimana et al. (2015), confidentiality can be achieved through proper classification, labeling, indexing, and file naming among others. Organisations including Moi University must ensure that those that have appropriate access to e-records handles them correctly (Bey 2012). Asogwa (2013) concludes that only authorised personnel should have access to information; thus, preventing information from being stolen or damaged. This would ensure the protection of e-records and consequently prevent disclosure of information that could harm the organisation or infringe on the privacy of individuals.

E-records integrity: Observing integrity is vital in the organisation for it ensures that e-records are accurate and remain unchanged representation of the original transaction (Bey 2012, Antirion 2011, Wu 2009, Bhaiji 2008, Parker 2002; Parker 1998). According to the Parkerian Hexad Model, integrity means information cannot be modified without authorisation. In e-records security management, breach of integrity can be displayed in many ways. For instance, when an employee accidentally or with malicious intent deletes important e-records when a virus infects a computer, when an employee can modify his/her salary in payroll, and when an unauthorised user vandalises a web site among others. ISO 15489-1:2001 explains that it is necessary that a record is protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised, and who is authorised to make them. Any authorised annotation, additions or deletion to a record should be explicitly indicated and traceable. Furthermore, ISO 15489-1:2001 suggests that control measures such as access monitoring, user verification, authorised destruction, and security should be implemented to prevent unauthorised access, destruction, alteration or removal of records to maintain integrity.

E-records availability: E-records availability component ensures that the e-records concerned are readily accessible to the authorised users at all times (Bey 2012; Antirion 2011; Wu 2009; Bhaiji 2008; Parker 2002; Parker 1998). Many authors have asserted that availability is the most challenging component to protect though it has not been given extensive attention (Qadir and Quadri 2016; Bey 2012; Martin and Khazanchi 2006). Unauthorised denial of use of e-records or information system could have a severe or catastrophic adverse effect on the organisational operation's assets or stakeholders (Dardick 2010). Availability of e-records dictates reliability, accessibility and timeliness of e-records and the systems that hold them. Frank (2016) concurs that an organisation shall maintain records in a manner that ensures timely efficient and accurate retrieval of needed information. This implies that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems always aim to remain available, preventing service disruptions due to power outages, hardware failures and system upgrades (Yinka n.d.).

E-records authenticity: Authenticity ensures the validity, trustworthiness, and dependability of e-records (Bey 2012; Antirion 2011; Wu 2009; Parker 2002; Parker 1998). It involves proof of identity (Clemmer 2010). DoD 50152 defines authenticity as a condition that proof that a record is genuine based on the mode (including method by which a record is communicated over space or time), form (that is format or media that a record has upon receipt), state of transmission (that is the primitiveness, completeness, and effectiveness of a record when it is initially set aside after being received), and manner of preservation and custody. Hence, authenticity aims to prove that a record is what it purports to be and that it had been created by the organisation with, which it is identified (Raaen 2017; Mukuevho and Jacobs 2012; Ismail and Jamaludin 2009). ISO (2001) states that an authentic record is one that can be proven to have been created or sent by the person purported to have created or sent it, and to have been created or sent at the time purported. The use of digital certificates and digital signatures is used to secure the authenticity of e-records (National Archives and Records Services of South Africa 2006). Like many organisations and institutions, Moi University has the responsibility of ensuring that authenticity is observed to enhance its reputation. ISO 15489-1:2001 asserts that an organisation should implement and document policies and procedures which control the creation, receipt, transmission, use, maintenance and disposal of e-records to ensure that records creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use, and concealment.

E-records possession or control: Possession or control of e-records refers to the ownership or control ability to use e-records (Bey 2012; Antirion 2011; Wu 2009; Parker 2002; Parker 1998). Parkerian Hexad Model defines possession or control as a state of having or taking into one's control or holding at one's disposal, actual physical control of property by one who holds for himself, as distinguished from custody, something owned or controlled. It is the attribute that describes the physical relationship between users and their technology. The growth of nomadic computing (driven by the new generation of cell phones, high sale of laptops, IPad, internet cafes, WiFi; and other growing specialised and inexpensive internet access devices as indicated in section 2.2.4), with its increased levels of non-local specific access via relatively small portable devices has increased the significance of this attribute. Possession or control is also about user rights management. Reid and Gilbert (2011) assert that another area of interest in the possession or control is digital rights management where the user or creator of information wants to maintain some ability to control its use or production. Subsequently, Possession or control is a vital component because it covers breaches where confidentiality is both critical and nonexistent. There are several ways of protecting e-records when a laptop, a mobile phone, hard disk or/and flash disks have been stolen or lost. For instance, cryptography is one powerful way of guarding against breach of confidentiality (Bey 2012).

E-records utility: E-records utility refers to the usefulness of information (Bey 2012; Antirion 2011; Wu 2009; Parker 2002; Parker 1998). ISO 15489-2001 explains that a usable record is one that can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records the document a sequence of activities should be maintained.

3.7 Skills and competencies available for e-records security management

To carry out the functions of any given job one must have appropriate competencies and skills to achieve efficient and effective output. The University of Toronto (2013) explains that competencies and skills can be supported by evidence of professional affiliation from a recognised organisation related to one's subject area.

The advancement of information and communication (ICT), its application and the abundance of software and hardware in the market have contributed to the proliferation of e-records. As early as 2000s authors have advocated repeatedly for the importance of capacity building in the area of information and records management (Cook 2006; Wamukoya and Mutula 2005; ICA 2004). Cook (2006) reiterates that information professionals need to realise that an utter transformation is taking place in the world of information; this, in turn, requires an entirely new paradigm or intellectual framework to situate our ideas and practice. Consequently, the trend with which technology is advancing, governments should be alert in terms of maintaining and upgrading infrastructure and equipping the personnel with required skills; This is because, the challenges brought about by the new advancement in technologies and e-records security management require that creators and managers of e-records be equipped with new skills and competencies through training and retraining to be able to effectively and efficiently operate and undertake projects in e-records management (Kumar and Bansal 2014; Ngoepe 2014; Nengomasha 2013; Asogwa 2012). Eiring (2008) on his part in a presentation at the International Council on Archives Congress in Kuala Lumpur, Malaysia asserted that the advent and the explosion of the creation and use of e-records demanded new technologies and methods of education and training on how to effectively and efficiently manage these records.

Similarly, Wamukoya and Mutula (2005) in their study on capacity–building requirements for e-records management in East and Southern Africa noted that various skills are required by records management staff. These skills and competencies are diverse but can be categorised into records and information management skills, technological skills, managerial skills, and project management skills. They further stated that other skills and competencies include, but are not limited to those needed to create, capture, classify, index, store, retrieve, track, appraise, preserve, archive and dispose records in an electronic environment.

The Parkerian Hexad model emphasizes that human resources are vital on the one hand and the biggest threat on the other to e-records security. For instance, the model explains that staff can sometimes enter inaccurate information, save over the wrong file, edit the wrong file, steal or share confidential information, intrude and accidentally delete files. For this reason, they should have competencies, skills and be provided with capacity building opportunities to enable an institution or organisation to achieve confidentiality, integrity, availability, authenticity, control, and utility of e-records (Parker 2002; Bey 2012). These sentiments are also echoed by the public service of Kenya (2010) that training and capacity building is critical for records management officers in the public service.

E-records are vital organisational asset and organisations depend on accurate, complete, readily available information to assist in making decisions, providing litigation support, improving organisational efficiency, documenting compliance with legislative, regulatory, contractual requirements and providing historical references (ARMA 2017; Asogwa 2013; Asogwa 2012; Luyombya 2010). The growing use of e-records has signaled the need for senior management, directors, records managers, records staff and action officers among others who are responsible for the e-records creation and use to be equipped with appropriate training (Johare et al. 2013; ISO 2001). The continuum model provides knowledge and skills that extend the concept of the continuum beyond metaphor (Upward 2004). In addition to the competencies outlined by the continuum model, understanding the organisation's business activities, objectives, and process; and classification of records skills are needed. Moreover, preparing disposal authorities, system designs; information management; technological management; human resource management and project management are essential skills and competencies in e-records security management (Wamukoya and Mutula 2005; ISO 2001). These competencies and skills are needed to manage e-records from creation or receipts through processing, distributing, sharing, using, accessing and securing, organising, storing, retrieving and disposing them.

As indicated in section 3.5, the Moi university responsibility of e-records security management is distributed among the individual units with little or no centralised control (Bigirimana et al. 2015; Kyobe et al. 2009). This implies that competencies and skills to all employees are mandatory to enhance e-records management security effectively. Ohio State University (2013) in this regard notes that the creating unit must actively maintain active records systems that have continuing utility and value. Maintaining these systems will entail routine system backup and may involve periodic or scheduled recopying of data from old to new storage media. Continued maintenance of electronic systems may require the responsible personnel migrate records considering their integrity to new systems that can take advantage of the most current systems and software. Competencies and skills in e-records security management and implementation of ICT services and systems and for the use of these systems are very limited in both academic and administrative areas. Consequently, staff training in the use of ICT services and systems, development of the ICT professional skills and appropriate management capacity are regarded as high-priority goals of the University (Moi University, ICT policy 2011).

Mnjama and Wamukoya (2007) observed that the level of awareness and commitment of staff could be used to gauge where an organisation is placed in terms of records management readiness on a scale of 1-5: Level 1-senior management has no understanding of commitment to the management of the organisation records; Level 2-senior management has a broad understanding of and recognise the need to embrace and support records management in the organisation; Level 3-senior management is highly committed to and are supportive of a records management programme in the organisation; Level 4- senior management has created an environment where records management is highly valued as part of the organisation's overall information management strategy and Level 5- the organisation is recognised for its stewardship and leadership role in implementing records management programmes.

ISO (2001) also asserts that organisations may choose to use already–trained staff to facilitate attendance by other staff at suitable external training programme or they may choose to engage trained and experienced consultants. ISO further explains that an organisation should consider the following methods of training: in-cooperation in organisations employee orientation programmes and documentation; classroom training for employees new particular responsibility at times of system change; on-job training by knowledge supervisor; training courses provided by educational institutions or professional organisations that may be part of the general offerings of these institutions or may be part of the general offerings of these institutions or may be developed on request to meet an organisation's particular needs; computer-based presentations which may be interactive, available on the network or storage device, workshops and seminars on-e-records security management issues and initiatives; and leaflets and booklets providing 'how to' guides describing aspects of the organisation’s record policies or practices. According to the Kenya public (2010) and ISO (2001), organisation, ministries, public institutions should employ personnel with professional qualification and should ensure that they continuously organise training in order to improve their competencies, knowledge, skills, attitudes, and ability to assimilate new technology to enable them to undertake the reforms in the records management function effectively and efficiently. Despite this directive, many scholars and authors have lamented about the inadequacy of appropriate competencies and skills in e-records management and security management in organisations and institutions (Musembe 2015; Ngoepe 2014; Nengomasha 2013; Erima 2013; Asogwa 2012; Sichalwe, Ngulube, Stilwell 2011; IRMT 2009; Kemoni 2008; Kemoni and Ngulube 2008; Wamukoya and Mutula 2005; Katuu 2004). Fourteen years ago International Council of Archives maintained that e-government services delivered using ICTs, will be compromised unless the issue of capacity building is addressed, noting that failure to address this issue could lead to reduced government effectiveness, increased operating costs, gaps in recorded memory, reduced public access to entitlements, erosion of rights, and weakened capacity for decision making (ICA 2004).

3.8 Strategies for sound e-records security management

Mutula (2013) observes that developed countries have all prioritised initiatives, such as the creation of enabling strategies within the parameters of the local context, alternative public information delivery methods, a focus on a common set of goals for the government agencies, enlisting senior management support, ensuring supportive telecommunications policies, promoting citizens involvement in policy formulation and the alignment of technology with development programmes.

In contrast, developing countries are just starting to appreciate the expansive and dynamic nature of ICT and the threats that come with it. For instance, the Kenyan government is starting to address the challenges of e-records security at the national level after realising that economic growth is in part predicated on the protection of competitive information (Ministry of ICT, Kenya 2014). Harris (2009) argues that achieving success depends on successfully sharing meaningful information within parts of the organisation. Modern ICTs when properly harnessed will contribute towards eliminating technological and system threats, which expose the organisation to dangers of delayed access to required information.

Kemoni (2009) asserts that to manage the e-records effectively in the East, Central and Southern Africa region, there is the need for governments and directors of National Archives within the region to implement recommendations proposed by various records and archives management researchers, scholars and practitioners. These recommendations include developing and implementing relevant records management policies and procedures, staff training in ICT skills, adopting e-records models, records and archives department working closely with ICT departments, upgrading ICT skills of staff, legislation to protect e-records, providing adequate funding for e-records management, using appropriate document management strategies and investing in more ICT infrastructure (Nengomasha 2009; Kaekopa 2007; Kemoni 2007; Wamukoya and Mutula 2005).

In order to strengthen e-records security management in an organisation, it is essential to understand and rank threats in order to give priority accordingly to the threats and the systems that create/receive, store, maintain, process and transmit the e-records. There are several security strategies that can be employed to safeguard e-records such as installing and updating virus software, using firewalls, authenticating access, using security software, encryption, and use of public key (Ngulube 2010; Magi 2008; Katuu 2004). Tasmanian Archives and Heritage Office (2015) adds that physical security, password creation and protection, intrusion detection and prevention security classification labeling, encryption, security shredding and information security awareness as measures that can be used to protect e-record assets. The government of New Wales notes that it is essential for the universities to back up e-records on a regular basis to safeguard against loss of information due to equipment malfunction, human error, or other disasters. The backup routine should target the most critical e-records. Bennett (2011) adds that organisations should consider digital signatures, encryption of portable storage media, backup of the records and cloud computing as a records security measure. Kabata (2013) in his study on outsourcing records storage to the cloud, challenges, and prospects for African records managers and archivists, opined that, in a cloud environment, storage of records or information is outsourced to a third party provider and accessed by the organisation through a network connection. The author further states that established cloud providers dedicate resources to improve their network and application security process. They use defensive measures such as patch management, hardening of virtual instances and virus scanning, which can be implemented quickly across the cloud provider's infrastructure through use of virtualisation and automation which allows replication of security.

During the year 2017, the government of Kenya enacted the computer and cybersecurity bill to provide for offenses relating to computer systems; to enable timely and effective detection, investigation and prosecution of computer and cybercrimes to facilitate international cooperation in dealing with computer and cybercrime matters; and for the connected purpose.

In addition, audit trail is a security strategy that should be applied to ensure that procedures are being followed, controls are applied correctly, and a record is preserved and accessible. Audit trails provide a chronological record of system activities that document the sequence of changes and activities that impact records such as changes to record content and context (ISO 2001). However, ICA (2008) is of the opinion that audit trails should be captured for all actions on the system and any changes to records must be documented. Besides, security should be enforced at all levels of e-records processing, folder, and system levels. It should also be enforced across the online information transmission lines to protect the records against online threats like eavesdropping and information hijacking.

As explained in section 3.7 capacity building, competencies and skills are strategies to threats in e-records security, and personnel are known to be the weakest link in e-records security management chain and continue to pose the greatest security threat to e-records. Despite having in place sophisticated hardware and software security, most organisations including Moi university seem unable to stem employee against sharing of passwords, making conscious or unconscious errors, deleting, altering, opening folders over the other, and posting confidential information on social media (Marutha 2016; Asogwa 2012; Bey 2012; Parkerian model 1998). For this reason, training and awareness should be mandatory and given priority regularly. Besides, vetting of staff, incentives, sanctions, and penalties should be implemented as a way of enhancing e-records security management (Kenya Computer and Cybercrime Bill 2017; Kenya Cyber Security Report 2015; Parker 2002). Standards, policies, and regulations are also essential strategies in ensuring e-records security management to enhance the creation and management of authentic, reliable and usable records (ISO 2001). Ngoepe et al. (2010) add that an effective policy framework can form the basis for policy guidelines aimed at fighting cybercrimes, controlling access to information, planning for business continuity, complying with legal and policy requirements, developing and maintaining in-house software, controlling e-records transaction, detecting and responding to information security incidents and classifying information.

Additionally, organisations should develop and enforce policies and guidelines on e-records security management including creation and maintenance, access, access control, access privileges, security classification, appraisal, retention, and disposal (Marutha 2016; Asogwa 2012; Marutha 2012; Mishra 2011; Sichalwe et al. 2011). ISO (2001) sums that organisations should ensure that the policies are communicated and implemented at all levels in the organisation (ISO 2001).

3.9 Summary and Gaps in the literature

The chapter reviewed literature of related topics to e-records security management from general to specific (Creswell 2014). The literature reviewed has provided useful insights and provided the foundation for the current study. Many studies in the field of e-records management have been conducted nationally and internationally. The literature reviewed above has addressed among others: e-records management essential components, characteristics of e-records, reliability, retrieval and authenticity, audit trails, classification, training and capacity building of records management, cybersecurity and challenges facing organisations in managing e-records in developed and developing countries. The literature review was organised thematically using themes gleaned from research questions, theories underpinning the study and the broader areas of the study. The themes included e-records records management, security classification of e-records process handling to facilitate description and access control, security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated, measures available to protect unauthorised access to e-records, how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved, skills and competencies available for e-records security management.

The literature has underlined the importance of e-records management through the entire continuum from the point when they are created or received through their inactive life to the point of retention indefinitely for legal, fiscal, administrative or historical reasons until their disposal which could be destruction or preservation as a permanent record. Moreover, the literature has indicated that adopting the use of ICT in e-records is often not well planned. The inadequacy of policy framework, funding among other challenges hinder organisations from sound e-records management. The literature reviewed seems to fall short in putting emphasis on e-records security management. It would appear in many organisations including Moi University, security appears to be considered after records are created, received, used and during storage. This should not be the case as the process of records lifecycle and security considerations should be inextricably intertwined. For instance, business process analysis should be a basis of identifying business processes and e-records and their value which should dictate legal restrictions or any other restrictions, as well as considering the impact of cyberspace in the management of e-records. Therefore, developing e-records security classification guideline as a basis of e-records security management to allow processes to pass through each other simultaneously and seamlessly is vital. The study, therefore, seeks to demonstrate the importance of aligning security and management of e-records.

This study therefore sought to address this gap by providing a platform for processes, controls, policy and regulatory regime for e-records security management in order to enhance integrity, accountability, transparency and ethical conduct in records management, and also provide the framework for staff training and infrastructure development to enhance e- records security management at the Moi University. To accomplish this task, the study therefore aimed at answering the following research questions: How are e-records created, maintained, stored, preserved and disposed? How is security classification of e-records process handled to facilitate description and access control? What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated? What measures are available to protect unauthorised access to e-records? How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved? What skills and competencies are available for e-records security management?

CHAPTER FOUR

RESEARCH METHODOLOGY

4.1 Introduction

Appropriate research methodology is required to conceptualise research problems and describe the phenomena that are being investigated (Ngulube 2015). Willis (2007) explains that methodology is used to describe several aspects of a study; the design, procedure for data collection, methods of data analysis, selection of subjects and details of the specific treatment, if any. From Willis explanation, research methodology is a plan or lens through which a researcher formulates various steps on acquiring knowledge and getting answers to the research problem. Ngulube (2015) acknowledges that knowledge that is produced in any scientific field primarily depends on the methodology that is used.

The main aim of this study is to investigate the e-records security management at Moi University and formulate strategies for improvement. The study addresses various research questions including How are e-records created, maintained, stored, preserved and disposed? How is security classification of e-records process handled to facilitate description and access control? What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated? What measures are available to protect unauthorised access to e-records? How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved? and What skills and competencies are available for e-records security management?

The chapter is organised around the following thematic areas; research paradigms, research approaches, research design, study population, sampling procedures, data collection techniques, data presentation and analysis, reliability and validity of the study, ethical consideration and summary.

4.2 Research paradigms

Polit and Beck (2008) point out that paradigms for human inquiry are often characterised in terms of how they respond to fundamental philosophical questions: ontological, epistemological and methodological. These philosophical questions are packaged in paradigms which guide everyday research (Savantakos 2013). Willis (2007) defines a paradigm as a comprehensive belief system, worldview or framework that guides research and practice in a field. Different paradigms lead researchers to ask different questions, use different methods to study those questions, analyse data in different ways, and draw different types of conclusions from the data.

Mackenzie and Knipe (2006) conclude that without nominating a paradigm as the first step in research, there would be no basis of subsequent choices on methodology and even literature. Therefore, paradigms are defined by the reality of things (ontology), knowledge of that reality (epistemology) and the tools used to know that reality (methodology) (Ngulube 2015; Anderson 2013).

There are three paradigms in which research is conducted; they include positivism, interpretivism, and pragmatic paradigms. The methodology of positivism is quantitative, interpretivism is qualitative, while pragmatic is mixed methods research (Ngulube 2015). Greenfield et al. (2007) explain that positivists believe that researchers can control their biases sufficiently and also control the environment enough to identify an objective truth that can be generalised into universal laws or principles, while interpretivism posits that it is necessary for the researcher to understand differences between humans in our role as social actors. That is, as social actors, we interpret our roles and those of others according to the meaning we give to those roles.

Ngulube (2015) asserts that the pragmatic paradigm was born out of an attempt to bridge the gap between interpretivism and positivism paradigms. Creswell’s (2003) view is that pragmatic paradigm is not committed to any one system of philosophy and reality. It draws from both quantitative and qualitative assumptions. In this case, researchers are free to choose the methods, techniques, and procedures of research that best meet their needs and purposes. Furthermore, it does not see the world as an absolute unity and truth, but what works at the time. Creswell concludes that it is not based on a strict dualism between the mind and reality completely independent of the mind.

4.2.1 Pragmatic paradigm

This study employed the pragmatic paradigm since it allows the application of qualitative and quantitative methods. Pragmatic paradigm is concerned with ‘what works' and solutions to problems rather than the methods used; in this case, researchers use all approaches to understand the problem (Creswell 2003). Mixing methods and techniques also enriched the study by enlightening facts that would otherwise be left out if only one method could have been used. Pragmatists believe that the truth is what works best for understanding a research problem (Ngulube 2015; Migiro and Magangi 2011; Patton 2002; Tashakkori and Teddlie 1998; Rossman and Wilson 1985). Pragmatic paradigm draws on many ideas including applying 'what works' using diverse approaches and valuing both objective and subjective knowledge (Cherry holmes 1992). Therefore, given that the pragmatic paradigm is concerned with what works, that solutions to problems are important than the methods used, and no research methodology is perfect, and that researchers must use data obtained with multiple methodologies, it was found suitable for this study.

Pragmatism also looks at how our values and ethics, politics and epistemologies and worldviews as researchers directly influence our actions and our methodologies (Morgan 2007). The choice of the paradigm in this study was also influenced by the fact that the field of e-records security management exists within technological, social and security context, which offers a new prospect to the third methodological movement (Teddlie and Tashakkori 2003), that of abduction-intersubjectivity-transferability, in which reasoning moves back and forth between induction/deduction and subjectivity/objectivity, just as pragmatist researchers actually do (Brownwynne et al. 2012; Morgan 2007).

4.3 Mixed Method Research (MMR)

The pragmatic paradigm is consistent and best paradigm for mixed method research where qualitative and quantitative aspects are employed (Ngulube 2015, Teddlie and Tashakkori 2009, Datta 1994, Howe 1988). Creswell et al. (2008) define mixed methods as the collections or analysis of both quantitative and qualitative data in a single study in which the data are collected concurrently or subsequently given priority and involve the integration of the data at one or more stages in the process of research. This implies that multiple methods may be used in a single study to take advantage of the representativeness and generalisability of quantitative findings and the in-depth, contextual nature of qualitative findings (Greene and Caracelli 2003). The researcher believed that mixing methods would enrich the study by revealing details that may have been left out if one method was employed in investigating e-records security management in Moi University. This also provided the possibility of the neutralisation of the weaknesses of one method and strengthening the benefits of the other for the best results. Creswell et al. (2008), Punch (2006), Martens (2003), Newman and Benz (1998) sum up the rationale of mixed method by stating that different methods can be used for different purposes in a study. For instance, a researcher may wish to employ interviews in order to get a feel for the critical issues before embarking on a questionnaire. Secondly, the approach enables triangulation to take place, which refers to the use of different data collection methods within one study in order to ensure that the data are telling one what they think it is telling them. That is, it facilitates the comparison of quantitative and qualitative data sets to produce a well-validated conclusion. Thirdly, the approach helps to explain quantitative results with subsequent qualitative data in order to develop a theory that is then tested. Finally, the multi-method enhances a study with a supplemental data set either quantitative or qualitative.

MMR can be conducted concurrently or sequentially (Moseti 2015; Sichwele 2010; Teddlie and Tashakkori 2009; Creswell 2003). Terrell (2012) and Creswell (2003) outline six major strategies used in MMR. They include: Sequential explanatory strategy (involves collection and analysis of quantitative data followed by the collection and analysis of qualitative data), sequential exploratory strategy (collection and analysis of qualitative data followed by the collection of quantitative data), sequential transformative (there are two distinct data collection phased out, and either type can be used to collect data first (priority can be given to either or both data types)), concurrent triangulation strategy (priority should be equal, but can be given to either approach), concurrent nested (there are two data collection methods, one is embedded (i.e., nested) within the other, and concurrent transformative strategy (priority may be given to either phase, or there may be equal).

The study adopted the concurrent nested strategy where quantitative and qualitative data were collected simultaneously. This was to mitigate on the inherent biases associated with using only one method when the researcher logistically cannot place equal priority on both primary and secondary types of data. Moreover, the concurrent nested strategy allow collecting of information from different groups or levels within an organisation thus gaining greater perspective than could be obtained from using either of the data collection method. Edmonds and Kennedy (2013) refer to this strategy as an embedded approach. They explain that the approach is used when different questions require different types of data when one data type plays a secondary role and would not be meaningful if not embedded within the primary data set and when the corroborated researcher logistically cannot place equal priority on both types of data. MMR has been used in related studies such as Maseh (2015) in a study on records management readiness for open government in the Kenyan Judiciary. Maseh employed the MMR in order to seek convergence and corroboration of findings through use of more than one method of gathering and analysing data; hence, eliminating the inherent biases associated with using only one method. Moseti (2015) in a study of strategies for managing scholarly content at the universities in Kenya, noted that mixed method research benefited the study leading to more research income, higher quality research, recruitment and retention of higher quality researchers and greater research output for the institutions. Luyomba (2011) in a study on a framework for effective public digital records management in Uganda, noted that the mixed method yielded an improved and elaborated understanding of digital records management collecting diverse types of data using different methods and thus, providing the study with a broader understanding of digital records management.

4.4 Research design

A research design is described as a blueprint or an overall plan according to which the initial set of questions are structured, respondents of a proposed study are selected as well as the means of data collection (Creswell 2013; Welwan et al. 2009; Babbie and Mouton 2008; Yin 2003). Macmillan and Schumacher (2001) define research design as a plan for selecting subjects, research sites and data collection procedures to answer the research questions. They further indicate that the goal of sound research design is to provide results that are judged to be credible.

This study employed a case study research design. MacMillan and Schumacher (2001) indicate that a case study examines a bounded system or a case over time in detail employing multiple sources of data found in the setting. All pieces of evidence are collected to arrive at the best possible responses to the research questions. As a result, the researcher may gain a sharpened understanding of why the instance happened and what might become important to look at more extensively in future research. The case study approach is especially useful in situations where contextual conditions of the events being investigated are critical and where the researcher has no control over the events as they unfold (Yin 2003).

By applying the case study design in this study, the researcher was able to answer specific research questions, which sought a range of different pieces of evidence from the case settings (Gillhan 2003). Although case study design has been linked with a qualitative approach (Barxter and Jack

2008), case studies can include and even be limited to quantitative evidence which may include questionnaires, interviews, observation and documentary analysis (Saunders et al. 2012; Yin 2003; Gilham 2000). Yin (2009; 2003) describes four types of case studies as:

i. Single case (holistic) design, where a single unit of analysis is selected to represent a unique or critical case. One selects a single case as a representative or one which has not been considered before.
ii. Single case (embedded) design, involves more than one unit of analysis within a single case. The sub-units have been found to add significant opportunities for extensive analysis, enhancing the insights into the single case.
iii. Multiple case (holistic) designs, is where a study contains more than a single case.
iv. Multiple case (embedded) designs, this involves several units of analysis within the multiple cases.

This study adopted the single case (embedded) design where an investigation of sub-units (top management, deans and directors, action officers, records staff and records managers) was undertaken to enhance extensive analysis and insights into the single case (Moi University). Given the pragmatic paradigm that was adopted in this research, the methodology (mixed method) of the research and the nature of the research questions, the single case study design was considered the most suitable approach to utilise because unlike other forms of research design, the case study does not utilise any particular methods of collections or data analysis (Merriam 1998). Also, the case study design provided a systematic way to collect, analyse data and report the results. It also helped in understanding the research problem in great depth. It also provided a variety of participant perspectives using multiple data collection techniques. Moreover, the choice of a case study design gave the researcher ample room to conduct an in-depth investigation of the unit of analysis (Yin 2009). This provided a significant amount of description and detail about the state of affairs in so far as e-records security management affairs at the institution are concerned.

The case study design also offered more opportunities for the researcher to gather adequate information to make accurate inferences at the end of the study and helped to set the groundwork for future studies (Orodho 2008). The case study design has been applied widely by different authors, for instance, Maseh (2015) in her study of records management readiness in the Kenya

Judiciary, adopted the case study design in order to develop a rich narrative and reveal records management practices in the Kenyan Judiciary. IRMT (2011) undertook a case study on managing records as reliable evidence for ICT /e-government in the Kenyan Judiciary. Some of the findings of the study showed a lack of skills and expertise in electronic records management and lack of government-wide records management policy.

4.5 Population of the study and sampling procedure

A population is a group of individuals sharing some common set of characteristics. Sichalwe (2010) describes a population as the universe of units from which the sample is to be selected. The population of the study consisted of one hundred and forty-five (145) respondents purposively selected from top management, deans and directors, action officers and records managers. The entire population was studied (census). The distribution of the population is shown in table 4.

Table 4: Population of Study

	Designation					
Department	**Top Management**	**Deans &Directors**	**Action officers**	**Records staff**	**Records Managers**	**Targeted Number**
Office of the VC	1	0	6	1	0	8
DVC Academic Research and Extension Office	1	0	2	1	0	4
DVC Finance Office	1	0	2	1	0	4
DVC Administration Planning and Development	1	0	6	1	0	8
DVC Student Affairs	1	0	2	1	0	4
Legal Office	1	0	1	1	0	3
School of Medicine	0	1	4	1	0	6
School of Public Health	0	1	4	1	0	6
School of Nursing	0	1	4	1	0	6
School of Dentistry	0	1	4	1	0	6
School of Engineering	0	1	4	1	0	6
School of Information Science	0	1	4	1	0	6
School of Business and Economics	0	1	4	1	0	6
School of Agriculture and Natural Resources	0	1	4	1	0	6

	Designation					
Department	Top Management	Deans &Directors	Action officers	Records staff	Records Managers	Targeted Number
School of Arts Social Sciences	0	1	4	1	0	6
School of Aerospace	0	1	4	1	0	6
School of Tourism, Hospitality and Events Management	0	1	4	1	0	6
School of Biological and Physical Sciences	0	1	4	1	0	6
School of Law	0	1	4	1	0	6
School of Education	0	1	4	1	0	6
School of Human Resource	0	1	0	0	0	1
Central Registry	0	0	0	18	5	23
Directorate of Information and Communication Technology	0	1	2	0	0	3
Directorate of Quality Assurance	0	1	1	1	0	3
Total	6	17	78	39	5	145

(**Source:** Moi University, Human Resource Department Staff List 2017)

From table 4, six (6) top management comprises Vice-Chancellor (VC), Deputy Vice chancellors, Student Affairs (SA), Finance (F), Academics, Research & Extension (AR&E), Administration, Planning and development (A, P&D), and Legal Officer.

Deans and directors comprised the Fifteen Deans (from the 15 schools in Moi University, see section 1.2): one (1) ICT director, and one (1) quality assurance director.

Furthermore, seventy-eight (78) respondents comprised the ICT personnel and senior administrative officers. It is noteworthy that the ICT personnel and senior administrative officers were classified under action officers' stratum. The ICT staff constituted (28) personnel drawn from the schools (2 per school), two (2) from the office of Vice Chancellor, one (1) from each of the four offices of the Deputy Vice-Chancellors and two (2) from ICT Directorate. The senior administrative officers included, twenty eight (28) from the schools (2 per school), four (4) from the office of the Vice-chancellor, one (1) from DVC academic, research and extension office, one (1) from DVC finance office, five (5) DVC administration planning and development, one (1) from DVC students affairs, one (1) from legal office and one (1) Directorate of quality assurance.

Moreover, thirty-nine (39) records staff, one (1) from each school, one (1) from the VC's office, one (1) from each of the four DVC's offices, one (1) from legal office, one (1) Directorate of quality assurance and eighteen (18) from the central registry. The population also comprised five (5) record managers from the central registry.

The top management at Moi University is responsible for formulating policies and procedures for the management of records. Besides, strategic planning, resource mobilisation, management, allocation and accounting for funds, review, and monitoring of decisions is approved by the university council (the top governing body of the University).

Deans and Directors at Moi University provide leadership for schools and directorates respectively. They have the ultimate responsibility of making recommendations to the university and interpreting and representing the work of the college to constituent schools and directorates outside the university. They also ensure high standards in the production and evaluation of program and activities of the school and directorates. In consultation with schools and directorates, they exercise leadership in the selection, retention, promotion, and development of school or directorates staff. They are also responsible for the management of resources and facilities.

The action officers (who comprised senior administrators and ICT staff), records managers and records staff, on the other hand, are responsible for records management from creation, use, maintenance, storage, and disposal. They also ensure the physical security of university human resources facilities and equipment, carry out internal audits and plans, oversee external audits on all University processes and keep records on all audits, both internal and external.

4.6 Sampling procedure

The study adopted a census sampling technique. Krishnaswami and Ranganathan (2010) state that when the population to be studied is relatively small described by Israel 2009, 1992, as 200 or less, the researcher may decide to study the entire population, referred to as census. Census eliminates sampling error and provides data on all the individuals in the population (Israel 2009; 1992). The total population for this study was 145 (see table 4.1). Therefore, this made a census sampling technique attractive (Israel 2009; 1992). As such, all the population was included in the study. To improve on the efficiency of the sampling, the population was classified into mutually exclusive strata; that is: top management, deans of schools and directors, records managers, action officers and records staff.

4.7 Data collection procedure

Given that the study was mixed method research, both qualitative and quantitative data were gathered simultaneously during a single phase of data collection, where the researcher believed that the resulting mixture or combination has complementary strengths and non-overlapping weaknesses. Questionnaires (see appendix 1) and interview schedules (see appendix 2 and appendix 3 respectively) were used as the primary sources of collecting data. The questions in the interview schedules and questionnaires were coined around thematic areas captured in the research questions and divided into different sections.

4.7.1 In-depth semi-structured interview

Kumar (2005) states that interviews are useful to obtain detailed information about personal feelings and opinions of people. Interviews provide the most appropriate means of engaging the participants to get a more detailed and in-depth description of the phenomenon. In this regard, semi-structured interviews were administered to the top management (see appendix 2), deans of schools and directors of directorates (appendix 3). Serem et al. (2013) indicate that semi-structured interviews still have some structure, which ensures that all major topics are covered, they are less formal and give interviewers more freedom to gather a wider range of information. They further indicate that semi-structured interviews allow probing of interesting issues and gathers much more detailed information on the chosen subject. Permission was earlier sought (see section 4.10) from the National Commission for Science, Technology, and Innovation (NACOSTI), which is the body that authorises research to be conducted in Kenya. Approvals were also granted by the county commissioner and authorisation of the county director of Education in Uasin-Gishu County where Moi University is located. Moreover, permission was sought from Moi University. After receiving full approval from UKZN, Humanities & Social Sciences Research Ethics Committee on 7th March 2018 to collect data (see appendix 10), the researcher immediately commenced the data collection exercise. The interviews were carried out at Moi University from 15th March to June 2018. The researcher conducted the interviews in person. The interviews were conducted in the interviewees' respective offices. The interview sessions lasted an average of (45) forty-five minutes each.

The data was collected on e-records practices, policies and legislative frameworks, ICT infrastructure, evaluation, and monitoring mechanism that ensure functionality of ICT and e-records management security infrastructure, budgetary provisions, place of e-records management in the organisation structure, e-records security plan, staffing, and training.

4.7.2 Questionnaires

Questionnaires are the most used and common data collection instrument in research studies. According to Fowler (2002), designing a questionnaire involves selecting the questions needed to meet the research questions of the study, testing them to make sure they can be asked and answered as planned.

The researcher and research assistants visited all the targeted respondents in schools and departments involved in the study in person to deliver the approval letters (see appendix 7, 4, 5 6 8), and informed consent letter (appendix 9). The approval letters and informed consent were important and necessary as an indication of the strict adherence to the ethical considerations of the measures taken to maintain human dignity, while gaining knowledge from the research. The researcher then administered the questionnaires with the help of research assistants to the respective targeted respondents. To ensure high response rate, the researcher frequently reminded respondents through phone calls and planned official visits and social calls. As a result, it took an average of three weeks for the respondents to complete and return the questionnaires. As indicated in section 4.7 data (qualitative and quantitative) were gathered simultaneously during a single phase of data collection; the questionnaires were distributed at Moi University from 15th March to June 2018.

Questionnaires (see appendix 1) were administered to action officers, records managers, and records staff. The questionnaires covered records creation, appraisal and disposal, security classification, security measures of e-records, maintenance and preservation of e-records, ethical values, physical security, training and awareness, and security threats. The type of questions included categorical data (see appendix 1; questions iv-vii, 17, 30), open-ended questions (see questions viii, 1, 2,3, 4 5, 6, 7,9, 10, 15, 17, 21, 22, 23, 24, 25,28,29,31) that led to probing of interesting issues and gathering much more detailed information on the chosen subject, closed-ended questions (see question 8, 13,14, 27), multiple response questions (see question 4b, 18, 20,30) and Likert scale questions (see questions 11, 12, 16, 19).

4.8 Data analysis

A mixed method approach was used to analyse data. According to Ngulube (2015), MMR combines the strengths of the qualitative and quantitative methodology to produce comprehensive and broad-based research. Ambira (2016) and Ngulube (2015) opine that qualitative research tends to generate an extensive amount of data even though few sources are consulted. Dawson (2009) suggests four approaches to qualitative data analysis: thematic analysis, comparative analysis, content analysis, and discourse analysis. Qualitative data were subjected to thematic analysis in this study. It involved coding, grouping the data into categories, identifying the themes and relationships among the categories in which the major themes that emerged from the data were compared to determine the pattern of association. For example, e-records like receipts, imprest, and Local Purchase Orders (LPOs) were categorised into accounting records. Furthermore, through verbatim reporting, codes were used to conceal the identity of the respondents, for instance, R7 in reference to a particular respondent. Thematic analysis is recommended for qualitative data by numerous authors including Ambira (2016), Ngulube (2015), Anderson (2010), Williamson et al. (2013), Clarke and Braun (2013), Burnard et al. (2008). On the other hand, quantitative data from questionnaires were analysed using Statistical Package for Social Sciences (SPSS version 24) and the results were presented by use of descriptive statistics such as means, frequencies, percentages, graphs, tables, and bar charts.

4.9 Reliability and validity of the instruments

Reliability and validity are significant ideas and major concerns in research as they are used to enhance the accuracy and consistency of the assessment and evaluation of a research study (Tarakol and Dennick 2011). A research study is reliable when the findings are repeatable (Serem et al. 2013; Saunders et al. 2012; Babbie 2004). On the other hand, research is said to be valid when the conclusions are true or correct (McBurney and White 2010). Saunders et al. (2012) explain that reliability is the ability of the data collection techniques and analytic procedures to produce consistent findings if they are repeated on another occasion or if a different researcher replicated them. This sentiment concurs with that of Payne and Payne (2004) that reliability is the property of a measuring device for social phenomena (particularly in the quantitative methods tradition, which yields consistent measurement when the phenomena are stable regardless of who uses it, provided the underlying conditions remain the same.

To establish the degree of reliability, scholars have developed several different techniques, for instance, test-retest, split-half method, using established measures and parallel forms (Serem et al. 2013; Saunders et al. 2012; Krishnaswami and Ranganathan 2010). Serem et al. (2013) explain that in test-retest approach the same data collection instrument is used more than once, with the same group of people and the results compared statistically. As the same instrument has been used with the same group, theoretically, there should be a strong correlation (relationship) between the two data sets, so a statistical measure of the strength of the relationship between the two is calculated. The name of this test is the correlation coefficient, and in practical terms, a value of 0.3 - 0.7 is needed to regard the instrument as having sufficient reliability. Using established measures is another degree in resolving the problem of reliability. Serem et al. (2013) state that this involves the use of an instrument that has already been validated. On split-half method, Saunders et al. (2012) state that the questions are randomly split into two sets and responses from each set correlated with the other set and the two should measure the variable in question in the same way.

Validity, on the other hand, is the degree to which an inference, conclusion or measurement corresponds precisely to the real world and offers the best possible approximation of its truth. Thatcher (2010); and Kothari (2004) are of the opinion that validity is the extent to which the instrument measures what it is supposed to measure. This implies that whether research accurately measures the things that it is aimed to measure or how appropriate (close to the truth) the results of the research are (Gibbs 2012). According to Serem et al. (2013) there should be a clear relationship between the way a concept is defined, and the way it is operationalised. This measure aims to assess whether or not the relationship is well established, or whether there is a gap between the information that was sought, and the data collected.

There are a number of basic methods of testing validity (Serem et al. 2013; Saunders 2012; Yin 2003) including, construct validity (refers to establishing correct operational measures for the concepts being studied), internal validity (involves establishing a causal relationship between two variables that means certain conditions are shown to lead to other conditions), external validity (establishing the domain to which a study's findings can be generalised. It is concerned with the questions; can a study's research findings be generalised to other relevant settings or groups?) and content validity (the extent to which a measuring instrument provides adequate coverage of the topic under study. Pre-testing is an example of a technique used in content validation).

Reliability and validity of data collection tools was assessed in various ways. A pre-test was conducted at Kisii University (see appendices 8 and 11 respectively). This method is supported by Blanke and Simone (2009) who state that a pre-test should be done under circumstances that are similar as possible to actual data collection and with a population as similar as possible to those that will be involved in data collection. Casper and Peytchera (2011) observe that pre-testing involves a series of activities designed to evaluate an instrument's capacity to collect the desired data, the capabilities of the selected mode of data collection and the overall adequacy of the field procedures. The authors' further state that pre-testing takes place before the actual data collection to enable identification of errors and suggest ways of improving the instruments to achieve accuracy and consistency. The pre-test in this study used a randomly selected sample of 20 respondents in the category of records managers and action officers who were asked to complete the questionnaires. The researcher interviewed one Deputy Vice-Chancellor, one registrar, two deans, and two directors. Data collected were analysed to generate information for instance on appropriate use of language and logical flow of the questions that was used to refine the questionnaire.

The internal consistency of responses in the study was tested using the Cronbach alpha (α) statistics. The statistical test was applied to measure the internal consistency of responses for individual questions with multiple items in the questionnaire after the pre-test. Maseh (2015) and

Beck (2004) explain that the most widely used method of evaluating internal consistency is coefficient alpha or Cronbach's alpha whose normal range of values is between.00 and +1.00 and higher values reflect a higher consistency. Nunally (1978) states that a general rule for measuring Cronbach's should be above 0.7, which implies that there exists a high degree of internal consistency in the responses. Table 5 shows the Cronbach's alpha values for the item-total correlation coefficients. From the table, all the dimensions had alpha values above 0.7.

Table 5: Cronbach's alpha values

Items	Cronbach's Alpha
Inadequate policies and regulatory frameworks in records management and security.	.795
Lack of training and skilled workforce in ICT and records management.	.795
Ignorance of staff and low profile is given to records management.	.785
Lack of access control mechanisms and safekeeping of passwords.	.803
Inadequate regulations of defining and assigning e-records security management responsibilities.	.786
Lack of access control and tracking of e-records.	.789
Inadequate strategies in preserving e-records.	.798
Assuming that any information online is safe.	.798
Lack of disposal and retention schedules.	.788

The study also adapted questions from tools that have been used in previous related studies for instance, World Bank (2002) on E-records Strategy. The instruments were also availed for critical review by experts in e-records management for their comments and feedback (Saunders et al. 2012; Teddlie and Tashakori 2009; Polit and Beck 2004).

4.10 Ethical considerations

The UKZN research ethical protocol was complied with (see appendix 10). Besides, the researcher sought permission from Kisii University to carry out the pre-test study (see appendix 7), permission was also sought from National Commission for Science, Technology, and Innovation (NACOSTI) in Kenya (see appendices 4 and 5 respectively). Approvals were also granted by county commissioner (see authorisation stamp on appendix 5) and authorisation of the county director of Education in Uasin-Gishu County where Moi University is located (Appendix 6). Furthermore, permission was sought from Moi University (see appendix 8). In addition, informed consent was sought and obtained from respondents before the commencement of the study (see appendices 9 and 11). The respondents were asked to participate in the study voluntarily and were free to withdraw at any stage of the data collection if they so wished. Further turn it in software was applied to test for plagiarism as form of academic ethical consideration.

4.11 Summary

This chapter presented the research methodology. In particular, the chapter discussed research paradigms, research approaches, research design, study population, sampling procedures, data collection techniques, data analysis technique, reliability and validity of the study and ethical consideration. The next chapter presents the results of the study.

CHAPTER FIVE

DATA ANALYSIS AND PRESENTATION OF THE FINDINGS

5.1 Introduction

Data analysis is the process of bringing order by organising and bringing meaning to the collected data to respond to the study research questions. In this case, qualitative data from interviews (see appendix 2) was subjected to thematic analysis. It involved coding and grouping the data into categories, identifying the themes and relationships among the categories in which the major themes that emerged were compared to determine the pattern of association. On the hand, quantitative data from questionnaires (See appendix 1) was analysed using Statistical Package for Social Sciences (SPSS version 24) and tabulated by use of descriptive statistics such as means, frequencies, and percentages, and presented using bar graphs and tables.

The purpose of this study was to investigate e-records security management at Moi University. The study addressed the following research questions: How are e-records created, maintained, stored, preserved and disposed? How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved? How is the security classification of the e-records process handled to facilitate description, control, disposal, and access status? What measures are available to protect unauthorised access to e-records? What skills and competencies are available for e-records security management? What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated?

This chapter covers the following subject areas: response rate, biographical profile of respondents, respondents duties in the current position, research findings under the following themes: e-records life cycle; themes e-records life cycle; Security classification of e-records process handling to facilitate description and access control; security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated; measures available to protect unauthorised access to e-records; how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records are achieved; skills and competencies available for e- records security management.

5.2 Response rate

The response rates covered here are obtained from data collected through interviews and questionnaires.

The target number of respondents was 23; however, those reached for the interviews were 21 representing a 91.3% response rate. In particular, a 83.3% (5) response rate was achieved from top management and 94.1% (16) from deans of schools and directors of directorates as shown in table 6.

Table 6: Interview response rate

Target Group	Target number	Response rate	Percentage
Top management	6	5	83.3%
Deans and directors	17	16	94.1%
Total	**23**	**21**	**91.3%**

From questionnaires out of 122 sent out, 118 were duly completed and returned representing an 96.7% response rate. In particular, 100% response rate was achieved from the schools, while the office of the Vice Chancellor recorded a slightly lower response rate of 85.7%. The high response rate was achieved because the respondents at a given unit were few and reachable. The results are presented in table 7.

Table 7: Response rate from questionnaires

	Designation					
Department	**Action officers**	**Records staff**	**Records Managers**	**Total Returned**	**Targeted number**	**Response rate**
Office of the VC	5	1	0	6	7	85.7%
DVC Academic Research and Extension Office	2	1	0	3	3	100%
DVC Finance Office	2	1	0	3	3	100%
DVC Administration Planning and Development	6	1	0	7	7	100%
DVC Student Affairs	2	1	0	3	3	100%
Legal Office	1	1	0	2	2	100%
School of Medicine	4	1	0	5	5	100%
School of Public Health	4	1	0	5	5	100%
School of Nursing	4	1	0	5	5	100%
School of Dentistry	4	1	0	5	5	100%
School of Engineering	4	1	0	5	5	100%
School of Information Science	4	1	0	5	5	100%
School of Business and Economics	4	1	0	5	5	100%
School of Agriculture and Natural Resources	4	1	0	5	5	100%

	Designation					
Department	**Action officers**	**Records staff**	**Records Managers**	**Total Returned**	**Targeted number**	**Response rate**
School of Arts Social Sciences	4	1	0	5	5	100%
School of Aerospace	4	1	0	5	5	100%
School of Tourism, Hospitality and Events Management	4	1	0	5	5	100%
School of Biological and Physical Sciences	4	1	0	5	5	100%
School of Law	4	1	0	5	5	100%
School of Education	4	1	0	5	5	100%
Central Registry	0	15	5	20	23	87.0%
Directorate of Information and Communication Technology	2	0	0	2	2	100%
Directorate of Quality Assurance	1	1	0	2	2	100%
Total	77	36	5	118	122	96.7%

5.3 Biographical profile of respondents

The study sought to establish the gender, age group, education level, duration of years worked, and the staff managed. This assisted the researcher in identifying whether respondents were balanced in terms of their category.

The respondents who completed questionnaires and those interviewed were 139 (91.7%). Of these 84 (60.4%) were male and 55 (39.6%) were female. The gender distribution is summarised in table 8 below.

Table 8: Respondents' gender

		Frequency	Percentage
Gender	Male	84	60.4%
	Female	55	39.6%
	Total	**139**	**100.0%**

In addition, the respondent's age was sought. The findings revealed that 59 (50.0%) were in the age range of 20-30 years, 39 (33.1%) were in the age range of 30 - 40 years, 26 (10.2%) were between 40 - 50 years, 11 (5.1%) were between 50 - 60 years. Only 4 (1.7%) were above 60 years. Age-gender cross-tabulation revealed that more males were in the 30-40 age group with no female above the age of 60 years as shown in table 9.

Table 9: Respondent's age group and gender (n=139)

		Gender			
		Male	Female	Total	Percentage
Age category	20 - 30 Years	31	28	59	50.0%
	30 - 40 Years	23	16	39	33.1%
	40 - 50 Years	18	8	26	10.2%
	50 - 60 Years	8	3	11	5.1%
	Above 60 Years	4	0	4	1.7%
	Total	**84**	**55**	**139**	**100%**

Regarding the level of education of the respondents the results showed that PhD holders were 21 (15.1%), masters were 34 (24.5%), and undergraduates were 63 (45.3%). Diploma and certificate holders were lower at 4 (2.9%) and 19 (13.7%) respectively.

The study also sought to establish the respondents' duration in the current positions. The findings indicated that 19 (13.6%) had worked for 0 to 2 years, 65 (46.8%) had worked between 3 to 6 years, and 56 (40.3%) had worked in the current position for 6 years and above.

Data from the interviews with regard to the number of staff managed indicated that 2 (9.5%) managed between 1 and 50. 4 (28.6%) managed 200 to 250, 7 (33.3%) managed 250-300, while 8 (38.1%) managed 300 and above members of staff. The data from interviews are summarised in table 10.

Table 10: Number of staff managed by interview data (n=21)

Respondents count	**Number of staff managed**
2 (9.5%)	1-50
4 (28.6%)	200-250
7 (33.3%)	250-300
8 (38.1%)	>300

Findings from the questionnaires showed that 79 (66.9%) comprising 44 action officers and 35 records staff managed no staff, 22 (18.6%) covering 16 action officers and 6 records staff managed between 1 and 10 members of staff, 3 (2.5%) managed between 11 to 20 staff, 7 (5.9%) managed between 21 to 30 staff, 2 (1.7%) managed between 31-40. Moreover, 5 (4.2%) indicated to be managing more than 41 staff. The result is summarised in table 11.

Table 11: Number of staff managed by questionnaire data (n=118)

		Designation				
		Action officers	**Records staff**	**Records Managers**	**Percentage%**	**Total**
Number of staff managed	None	44	35	0	66.9	79
	1 - 10	16	6	0	18.6	22
	11 - 20	2	1	0	2.5	3
	21- 30	2	0	5	5.9	7
	31 - 40	2	0	0	1.7	2
	> 41	5	0	0	4.2	5
	Total	71	42	5	100.0	118

5.4 Respondent’s duties in the current position

Data from interviews showed that all the 21 respondents were involved in carrying out specific duties in their current position. The top management consisting five (5) respondents specified the duties: Office of the VC: providing and demonstrating leadership, integrity and the highest standards of professionalism to the university and the community at large, strategic and academic leadership and planning, legislative awareness and compliance, policy development and implementation, management of national and international relations, coordination and facilitation of the activities of the University Council and its standing and ad hoc committees, planning, administration and development of university activities, overall management of the academic and administrative affairs of the university, signing collaborations and memorandum of understanding. DVC Students’ affairs duties include, but are not limited to, coordinating and overseeing all activities that affect student's welfare such as accommodation, guidance, and counseling, and on-campus work-study programs. DVC administration functions include: planning and development; coordination and preparation of the university's academic, physical and human resource masterplans; provision of leadership in performance-based management through performance contracting, staff appraisal and rewards; implementation of the university's strategic plan and other operational plans; implementing activities and services so as to ensure the university’s vision mission and objectives are realised; liaising with the VC and other stakeholders on matters of the university's corporate planning; budgeting and investment matters; maintenance of the database on the university's academic activities, human and physical resource management. Duties of DVC academic research and extension include: academic (admissions, examinations, provide secretariat services to Senate and its committees' as well as deans and its sub-committees', and overseeing library and services), research (conferences, projects, workshops, inaugural and public lectures), teaching (timetabling, examinations, certificates and transcripts), development, implementation, delivery of the curriculum and administrative duties. Furthermore, the duties of the DVC finance involve financial advisory and control, budgeting process, implementing financial policies and procedures, overseeing and coordinating activities of procurement department, analyses of reports from internal audit office, recommendations, and counsel among others. In addition, the duties of Finance Officer who works under the DVC finance as well as member of top management include: maintaining a comprehensive accounting system for the university that ensures that all revenues, expenditures, assets and liabilities are adequately accounted for; implement specific accounting procedures followed by the university in accounting for its finances as required by the regulatory agencies; advice the university in handling accounting and reporting problems; recommends systems changes designed to improve financial reporting; provide the university management with accurate and timely information for efficient and effective decision making among others. The Legal Officer on the other hand, specified duties as representing the institution in court, preparing legal documents, drafting memoranda of understandings, advising the institution on legal matters among others.

Deans and directors (16, 100%) also specified their functions to include among others: developing and implementing quality assurance at all levels of the institution; ensuring responsible use of university ICT resources to support the university's mission of teaching, research and outreach services, curriculum development, supervision of staff, managing and accounting for school resources, organising workshops and seminars, representing the school in the university management, Senate and deans' committees, procurement of materials and equipment at the school, involved in recruitment process.

Data from questionnaires showed that majority of respondents are performing administrative duties as shown in the Table 12 below.

Table 12: Duties performed by the respondents (n=118)

		Count	**Percentage %**
Duties performed in the current position	Administrative	42	35.6%
	Compliance	5	4.2%
	ICT	32	27.1%
	Accounts	17	14.4%
	Security (Physical)	5	4.2%
	Procurement	1	0.8%
	Curriculum Administration	15	12.7%
	Welfare	1	0.8%
	Total	**118**	**100.0%**

5.5 Research findings

The findings of the study were structured into themes that were formulated from the research questions as indicated in section 5.1. The themes include e-records creation, maintenance, storage, preservation and disposal, confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved, security classification of e-records, measures available to protect unauthorised access to e-records, skills and competencies available for e-records security management, security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated.

5.5.1 E-records life cycle

Research question one sought to find out how e-records creation, maintenance, storage, preservation, and disposal is carried out at Moi University. Interview schedule (appendix 2) questions 1-7 interview schedule (appendix 3 questions 1-5), and questionnaire (appendix 1) questions 1- 11 covered the research question.

The data from interviews (21, 100%) indicated that e-records are created and received by all members of staff at different levels in different departments, schools, directorates, and units. Others' records are received from outside the university, including the communication from different government ministries and international institutions and organisations worldwide. The respondents further indicated that the e-records are generated as a result of a business process not limited to, but including teaching, research, community activities, finance, collaborations, planning, administration, and development. They also pointed out that e-records are maintained and stored and preserved on computers, external disks, servers, databases, and offsite storage. The e-records formats used included PDFs, MS office documents, videos and audio files, pictures, drawings, and the markup language used on the university website. Records generated in particular include staff records such as those pertaining to employment, staff development, appraisal reports, staff dependents, staff disciplinary issues, student records (such as population, certificates, transcripts, welfare and disciplinary measures, nominal rolls, class attendance), internal and external reports, minutes and other records of meetings including notices and agenda, collaborations and memorandum of understanding, contacts and agreements, tender records, legal records, medical records, inventory records, policy records, graduation records, performance contract reports, architectural e-records such as maps and building plans, financial records including grants, budgetary records, salary payment, among others. All the respondents reported that e-records disposal does not happen. The responses were summarised in the words of two respondents R6 and R2 respectively. R6 stated that:

> "*Moi University like any other institution creates, maintains, uses, and stores records. Preservation is a challenge in its ways but though we migrate records to different storage devices to avoid losing information. The records are generated from the activities carried out in the school for instance student registration, staff deployment, examinations, finance and accounting, graduation, and workshops. Moi University is undergoing a transition from paper to e-records, and this has brought about massive use of modern technologies for example computers, mobile phones, and social media.*
>
> *Nonetheless, the widely used tool in generating and capturing e-records are computers. Furthermore, the data captured is related to research work, human resource, records of assets, student records and mainly financial records for example payment of fees and other sources of funds. Moi University like any other institution create, maintain, use, and stores records. Though the records are not disposed."*

R2 on the other hand observed:

> That all university members' staff are involved in e-records management directly or indirectly, and we also receive records from different departments of the university and outside the university. This is because the e-records provide evidence of the university's functions, operations, decisions, procedures, collaborations, and developments. For instance, in monitoring and implementing of the strategic plan and other tactical plans through efficient and effective resource allocation, e-records are a source of evidence to prove that these activities have been performed. The e-records are maintained and stored on computers, external disks, servers, databases, offsite storage, but when it comes to disposal we have not done it yet. The activities we carry out varies, and they involve teaching, research, community activities, collaborations and more. The records generated include staff records, student records, nominal rolls, class attendance, reports, minutes, memorandum of understandings among others.

The study then sought to find out the roles played by the respondents (appendices 2 and 3 question 2) from creation to disposal. All the 21(100%) respondents reported to be custodians of their respective directorates and schools e-records and the principle people in charge of the activities and are involved in all stages in the e-records life cycle. One respondent R20 noted:

> "*E-records issue comes in terms of maintaining both academic and staff matters. We are the ultimate custodian of e-records from creation to disposal. The school has both paper and e-records. The e-records are created and managed on computers and servers and also external storage for example hard-disks which are used as back- up copies. We have different departments and each department creates its own records which they, later on, bring or forward to the dean's office."*

The study also sought to find out functions that are pertinent to e-records management from action officers, records staff and records managers. The multiple response question was analysed with dichotomy group tabulated at value 1 representing "yes". Responses from the questionnaires revealed administrative function to be most pertinent to e-records management at 113 (95.8%) cases representing 42.5% of the respondents, and compliance function reported 52 (44.1%) cases constituting 19.5% of the respondents. Security and welfare functions both reported 8 (6.8%) and 6 (5.1%) cases representing 3% and 2.3% of the respondents respectively. Table 13 below presents a summary of the rest of the findings.

Table 13: Functions of departments (n=118)

		Responses		
		N	Percent	Percent of Cases
Selected[a]	Administrative	113	42.5%	95.8%
	Compliance	52	19.5%	44.1%
	ICT	34	12.8%	28.8%
	Curriculum Administration	19	7.1%	16.1%
	Accounts	18	6.8%	15.3%
	Procurement	16	6.0%	13.6%
	Welfare	8	3.0%	6.8%
	Security (Physical)	6	2.3%	5.1%
Total		266	100.0%	225.4%

a. Dichotomy group tabulated at value 1.

The respondents were further asked the types of records created and the people who create them. Responses from the questionnaires on types of records that are created and the people who create them are summarised in table 14.

Table 14: Types of records that are created and the people who create them (n=118)

		Designation of the person creating the record			
		Action officers	Records staff	Records Managers	Total
Types of records that are created	Financial Accounting and Audit records	14	6	1	21
	Inventory records	16	0	1	17
	Safety records	5	0	0	5
	Staff records	0	0	2	2
	Administrative records	6	30	0	36
	Student records	11	3	0	14
	Procurement records	0	2	1	3
	Service delivery	1	0	0	1
	Estate records	0	0	0	0
	Legal records	1	1	0	2
	Others	17	0	0	17
	Total	**71**	**42**	**5**	**118**

Regarding the standard file formats available for e-records creation and capture, the result showed that 99 (83.9%) of the respondents indicated web, windows, video and audio files. They specified the formats as MS office formats, pdf, audiovisual and images. Also, 19 (16.1%) of respondents specified other formats such as e-mails, quick books, text files and database as shown in table 15.

Table 15: Standard file formats available for e-records creation and capture (n=118)

		Count	Column N %
Standard formats available for e-records creation and capture	Web and Windows-based formats	99	83.9%
	Others	19	16.1%
	Total	118	100.0%

Moreover, responses from the questionnaires on how e-records are created, integrated and accessed by different departments revealed that web and desktop applications are the most used to create, integrate and access e-record at 103 (87.29%). The web and desktop applications platforms were identified as: MS office application, e-mails, social media, mainstream media, shared desktop folders, databases, management systems, and the university website. In addition, 15 (12.71%) specified other forms of access such as flash disks, Hard Disk Drives (HDD), compact disks, Digital Versatile Disks (DVDs) and internet as presented in figure 8.

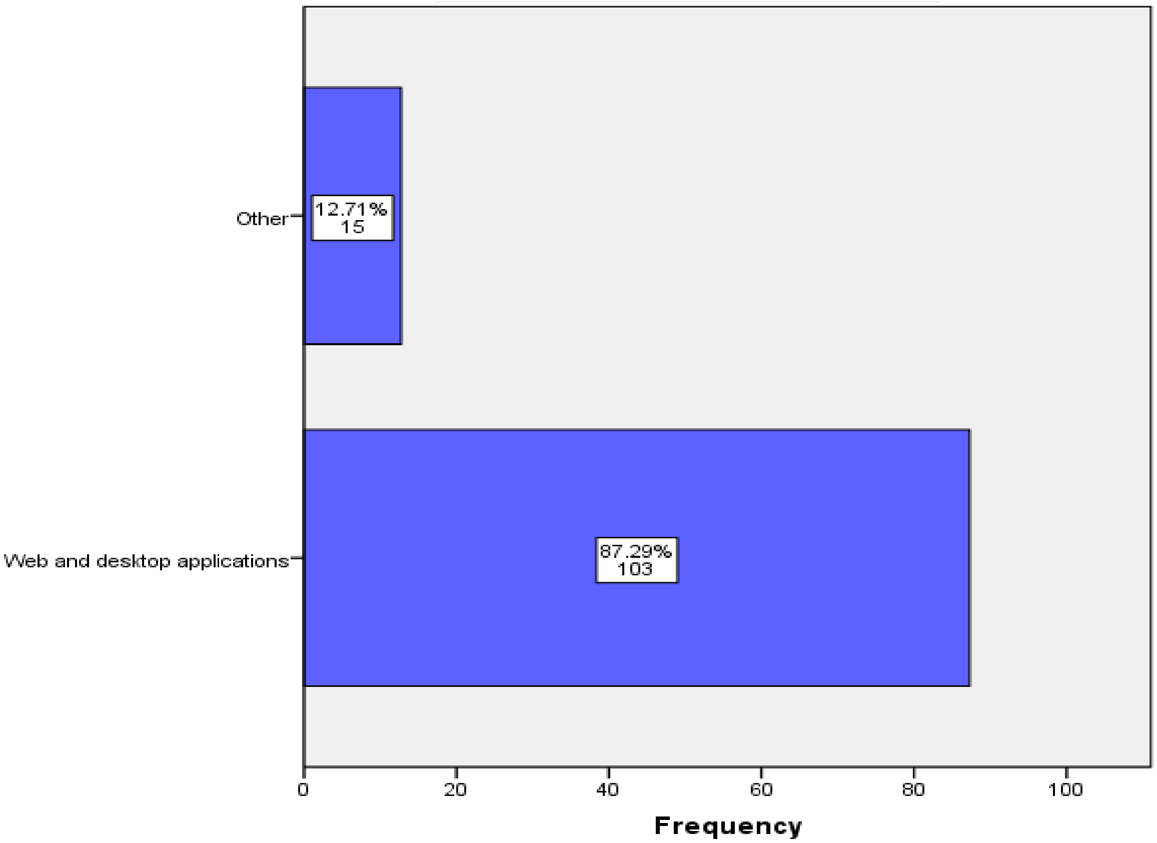


Figure 8: E-records creation and access by different departments (n=118)

The study sought to establish from action officers, records staff and records managers how e-records are maintained and stored. The results revealed that 107 (90.7%) of the respondents singled out desktop folders and external storage devices such as DVDs, flash disks, and external HDDs as means used for maintenance and storage of e-records. Only 11 (9.3%) mentioned online platforms such as emails and servers as other means of storage and maintenance as indicated.

The study also sought to determine the standard procedure in place for labeling storage devices from action officers, records managers and records staff. The results revealed that 85 (72%) respondents agreed that there exist standard procedures for labeling storage devices such as computer disks, flash disks, and external HDDs. The procedures and standards were identified as alphabetical, numerical, alphanumerical and classification as per subject. Furthermore, 19 (16.1%) indicated they were not aware whether such standards exist in the university, while 14 (11.9%) of the respondents were categorical that there existed no standard procedures for labeling storage devices.

The respondents were further asked designated areas available for the storage of active, semi-active and non-active e-records. The results showed that 24 (20.3%) of the respondents indicated online servers such as e-mails and database servers, 76 (64.4%) indicated desktop computers and external drives, i.e. desktop folders, external drives (hard disks, digital versatile disks, compact disks, flash disks) and the remaining 18 (15.3%) specified other platforms such as offsite and remote locations as designated areas available for the storage of e-records as reflected in table 16.

Table 16: Designated areas are available for the storage of e-records (n=118)

		Count	Percent
Designated areas available for the storage of active, semi-active and non-active e-records	Online servers	24	20.3%
	Desktop computers	76	64.4%
	Others	18	15.3%
	Total	**118**	**100.0%**

The results on measures that exist to ensure e-records remain accessible, authentic, reliable and usable through any system change during their retention were as follows: Computer security systems featured significantly at 43 (36.4%) that included; network security (antivirus and firewalls), regular updating of hardware and software and regular servicing and maintenance of the computers, authorised usage and access. Authorised usage and access followed at 36 (30.5%); restricted physical access of e-records through access/login credentials. Backup and recovery measures were at 20 (16.9%); backup in external devices (hard drive, digital versatile disks, compact disks, flash disks) with some stored in remote locations. Additionally, 19 (16.1%) of the respondents indicated measures classified as others; proper creation and maintenance of e-records, convenient and compatible processes and guidelines that are easily understood. A summary of the results are presented in figure 9.

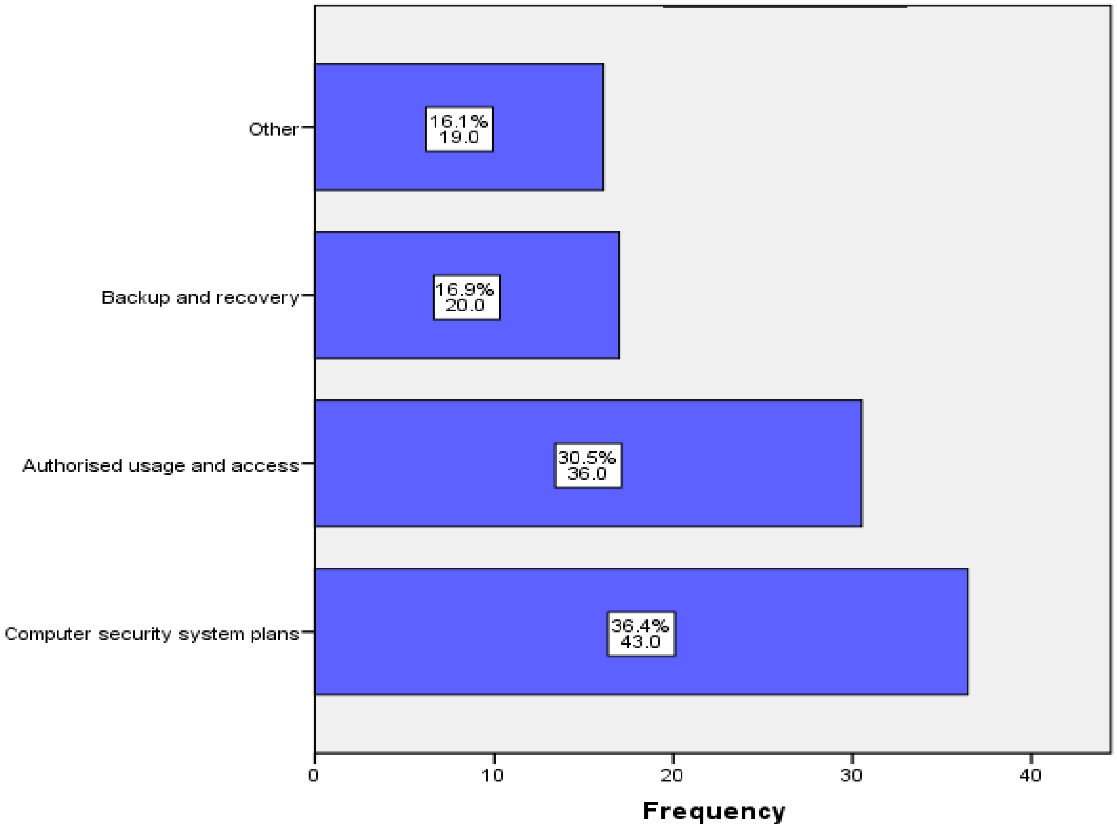


Figure 9: Measures to ensure e-records remain accessible, authentic, reliable and usable through any system change during their retention (n=118)

The study sought to find out the stage at which e-records are appraised and disposed. The results revealed that 2 (1.7%) of the respondents indicated that appraisal and disposal were done at creation, another 2 (1.7%) said appraisal was done at disposal. In addition, 23 (19.5%) were not aware at what stage appraisal was done, and 91 (77.1%) noted appraisal and disposal did not happen. The results are presented in table 17.

Table 17: E-records appraisal and disposal (n=118)

		Count	Percentage %
At what stage are e-records appraised	Creation	2	1.7%
	Disposal	2	1.7%
	Not aware	23	19.5%
	Not existing	91	77.1%
	Total	**118**	**100.0%**

On the criteria used to appraise e-records, data from the questionnaires showed that relevancy, reliability, sensitivity, usage, and age rated equally at 1 (0.80%), while 2 (1.7%) indicated nature of e-record is used as a criterion for appraising. Those who indicated the criteria did not exist were in the majority at 111 (94.5%). The results are depicted in table 18.

Table 18: Criteria used to appraise e-records (n=118)

		Count	Percentage %
Criteria used to appraise e-records	Relevancy	1	.80%
	Reliability	1	.80%
	Sensitivity	1	.80%
	Age	1	.80%
	Nature of the record	2	1.7%
	Usage	1	.80%
	Not existing	111	94.1%
	Total	**118**	**100.0%**

Moreover, the study also sought to establish the presence of structured disposal program and what it entails. The results revealed 2 (1.7%) reported the existence of a structured disposal program, 54 (45.8%), said they were not aware of the disposal program, and 62 (52.5%) said the disposal program did not exist as summarised in table 19.

Table 19: Presence of a structured disposal programme and what it entails (n=118)

		Count	Percentage %
If Moi University structured disposal programme and what it entails	Yes	2	1.7%
	Not aware	54	45.8%
	Not existing	62	52.5%
	Total	118	100.0%

As to whether the University has a retention framework, all the respondents reported that the university had no framework of ensuring the security of e-records at the disposal stage.

The study also sought to establish the respondent's view on the usefulness of a retention and disposal schedule. The results revealed that 7 (5.9%) reported that retention and disposal schedule gives guidance on the length of time for which records can be retained, 4 (3.4%) noted it helps in retaining core and e-records of enduring value, 6 (5.1%) said it ensures that records are available and useful for litigation, audit and day to day business purpose, 3 (2.5%) reported that it ensures the confidentiality, integrity of e-records, while 98 (83.1%) were not aware of the usefulness of a retention and disposal schedule.

The study further sought to find out strategies used for the preservation of e-records. According to 37 (31.4%) respondents, external drives backups are used as a strategy, 47 (39.8%) reported computer security plans, while 34 (28.8%) said authorised usage and access. The results are shown in figure 10.

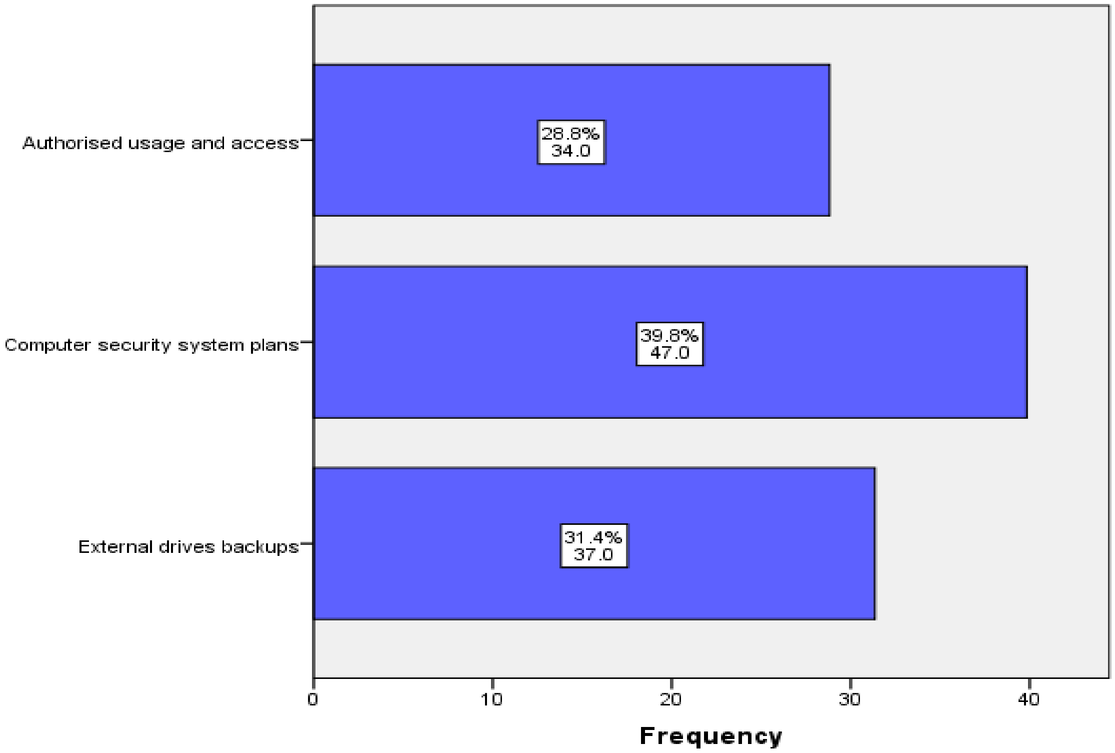


Figure 10: Strategies used for the preservation of e-records (n=118)

A significant number of respondents (81, 68.6%) reported having no idea about activities that are involved in administration and management of e-records throughout their lifecycle from creation to disposal. Figure 11 provides details of the results.

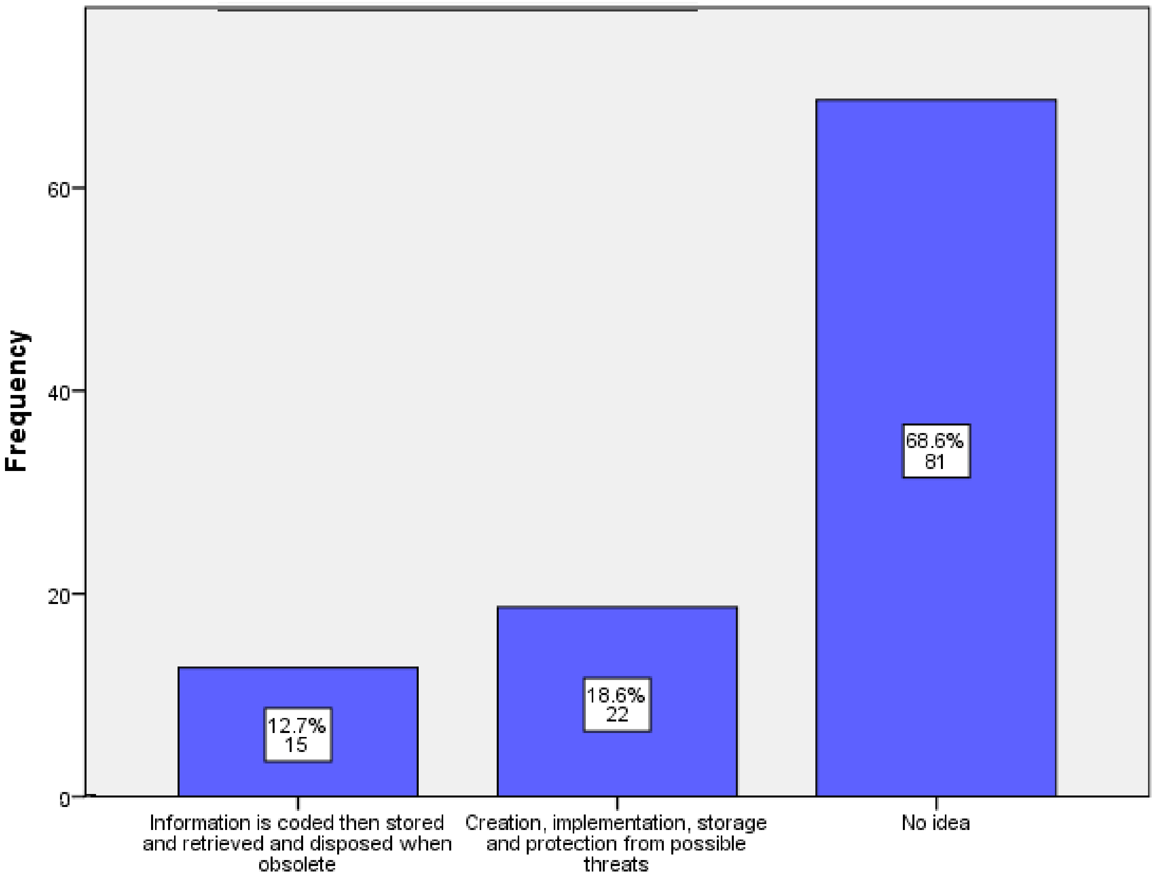


Figure 11: Activities in the management of e-records throughout their lifecycle (n=118)

5.5.1.1 Integration of e-record keeping functionalities into the university's business process

The study sought to understand how e-record-keeping functionalities are integrated into the business functions of the university (see appendix 1 question 6, appendix 2 question10 and appendix 3 question 5 questions). All 21 (100%) respondents interviewed were of the view that e-records management functionalities are not well integrated into the university business process systems. Instead, most of the e-records activities are carried out on single module systems and in office computers, as there are no policies in this regard — the respondents in accord listed the available systems as financial system, hostel management system, examination system, library system. The researcher went ahead to inquire if plans are underway of having a system that will capture all business activities, hence integrate record-keeping functionalities, 16 (76.2%) categorically indicated that they were not aware, while 5 (23.8%) indicated that there was a system being developed. The responses are summed up in the following responses of R6 and R3 respectively:

> *R6: "Integration is happening in a very haphazard manner despite the university gearing towards e-records management. There are no guidelines and policies. For example, when we are requested for information on staff and students, they ask for both hard copy and soft copy and what happens to the soft copy after it has been used is not known.*
>
> *Another example is that students have always been asked to submit both hard copy and soft copy of their projects and theses, but that is the end of it. Therefore, the integration should be more organised, structured and guided by a policy that will ensure that everybody is doing the right thing. There is a need for proper storage facilities, a central server and much training should be carried out for staff to understand more about the transition from paper to electronic. This is because integration is not just a mechanical thing but technical. The university needs to acquire the right systems, have policy frameworks and proper maintenance of systems for them to enhance e-records security".*

R3 observed:

> *We have not fully integrated our systems. In most cases, each division, department, and school create their e-records. However, the university is working on a system which will integrate all the activities of the university, for instance, human resource, academic affairs, and finance called IPPD. Though this was a call by the government years back for all governmental institution to develop and implement the system the university, has now heeded the directive to help enhance its functionalities. For the system has more modules including development and organisation of organisation structures, personnel cost planning and control that deals with monitoring of expenditure against approved personnel emolument budgets, personnel administration that deals with employee data to ensure compliance, payroll management and authorisation which deals with issues of security. The available systems, for instance, student accommodation system, finance system, and examination system can be accessed by individual schools and the finance department."*

Data from the questionnaires revealed 12 (10.2%) of respondents indicated that integration is done through classification of e-records, 23(19.5%) said it is done through accurate and timely labeling of storage devices, 17(14.4%) indicated authorised usage and access, while 66 (55.9%) were not aware of how the university ensures integration of e-record-keeping functionalities into business processes. The results are summarised in figure 12 below.

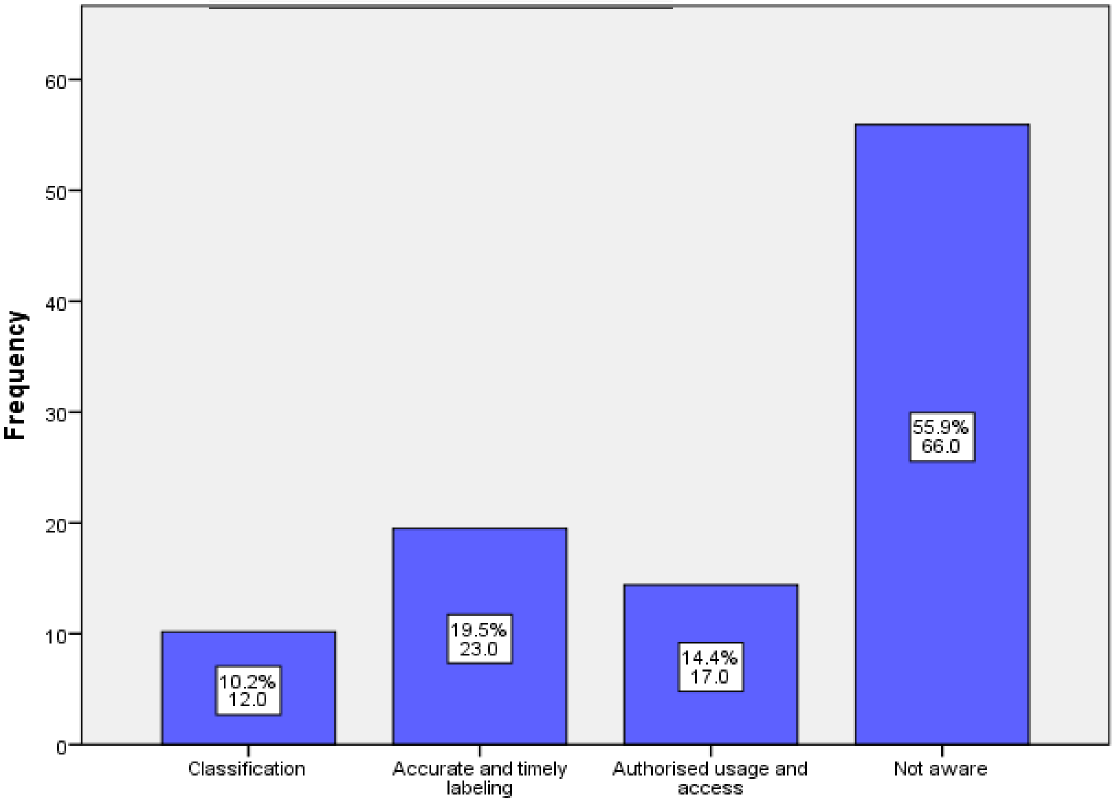


Figure 12: Integration of e-records keeping functionalities (n=118)

The study further sought to find out whether the available management systems meet all the e-records management functionalities (appendix 1 question 10). The findings showed that 9 (7.6%) reported that to a high extent management systems meet all e-records management functionalities, 34 (28.8%) indicated to a less extent, 32 (27.1%) indicated not at all, while 43 (36.4%) were not aware of extent to which the available systems meet all the e-records management functionalities. The results are depicted in table 20.

Table 20: Extent management systems meet all the e-records management functionalities (n=118)

	Frequency	Percent
Great	9	7.6%
Less	34	28.8%
Not at all	32	27.1%
Not aware	43	36.4%
Total	118	100.0%

5.5.1.2 Availability of policies guidelines or regulations and standards in records management and security

The study sought to know the available policies, guidelines or regulations that support e-records security management at Moi University (Appendix 1 question 7 and 11; Appendix 2 question11 and appendix 3 question 7). From the interviews, all 21 (100%) respondents indicated that there were no policies on e-records security management. However, 17 (80.9%) concurred that the ICT policy had been presented in one of the management meetings, which was to be implemented, while 3 (19.1%) said the policy was available but meant for general ICT and that the policy does not talk about e-records security management. The responses have been summed up in the following responses of R7 and R6:

> *R7: "We have a general ICT policy in soft copy that guides the university on all issues of ICT whether it is issues of security, management of information system, or e-records. However, we do not have a specific policy on e-records security or access. We are in the process of coming up with a specific security policy on e-records and other information generated in the university. That is one of the requirements of ISO/IEC 27001:2013 standard, and it is also part of our performance contract target for the next financial."*

On the other hand, R6 stated:

> *There is no policy on e-records management and e-records security management. The regulatory framework is expected to be national. In Kenya, e-records are admissible in a court of law and the government through the Information and Communication Act which recognises e-records. The framework by and large is there, but to make it lively, there should be a review of the Public Archive Act and the Public Archives and Documentation Act, which should be updated to explain very clearly and concisely the issue of e-records security management. The current Act talks about records in any form and does not talk about e-records which have hindered progress in providing solutions. The National archives that need to advise on the management of records is also short of workforce and skills, the government through national archives should inject more money for staff development. National archives should identify its priority that is training staff in e-records security management. Again, when talking about the regulatory framework, it involves guidelines, manuals developed by the national archives in setting out the fundamental challenges that e-records face, and the solutions and who is to provide the solutions."*
>
> *R3: "In addition to the ICT policy, the university has principal legal instruments governing the operations of university which include the constitution of Kenya 2010, the University Act 2012, No 42 of 2012, the Moi University Charter 2013, legal notice 2013, legal No 202 of 2013 and the statutes of Moi University 2013, and legal notice No 207 of 2013".*

The finding from the action officers, records staff and records managers indicated, 24 (20.3%) mentioned ICT policies, 30 (25.4%) said quality management procedures, while 74 (62.7%) were not aware of policies, guidelines or regulations supporting e-records security management.

The research further sought to find out the opinion of action officers, records managers and records staff on e-records management policies and regulations at Moi University. Generally, the results indicated that 42 (35.6%) of respondents strongly disagreed there was effective e-records management policies and regulations. Moreover, 57 (48.3%) of the respondents disagreed that policies and regulations are effective. A paltry 4 (4%) agreed, while 15 (12.7%) were undecided as shown in figure 13

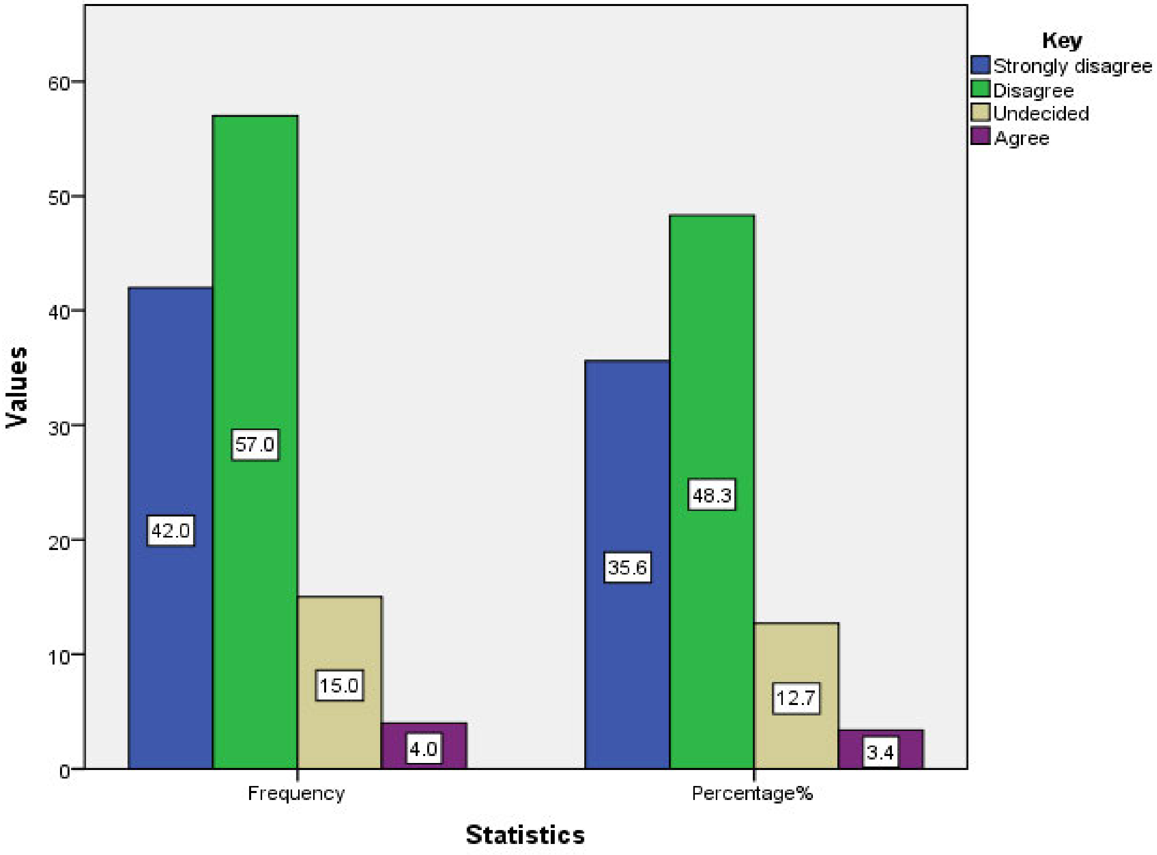


Figure 13: E-records management policies and regulations (n=118)

Itemised analysis of the assertions about the effectiveness of e-records management policies and regulations at Moi University is summarised in table 21.

Table 21: E-records management policies and regulations (n=118)

Assertions		Strongly disagree	Disagree	Undecided	Agree	Strongly Agree	Mean
The available policies and regulatory frameworks are adequate for the e-records security management	Frequency	42	57	19			2 (Disagree)
	Percent	35.6	48.3	16.1			
Lack of policies and regulatory frameworks have led to poor e-records security management	Frequency			19	42	57	2 (Disagree)
	Percent			16.1	35.6	48.3	
The available e-records policies and regulatory frameworks have been communicated at all levels of the University	Frequency	42	57	15	4		3 (Undecided)
	Percent	35.6	48.3	12.7	3.4		
The university management is on the forefront in promoting the application of records management policies throughout the University	Frequency	61	38	15	4		4 (Agree)
	Percent	51.7	32.2	12.7	3.4		
The available policies and	Frequency	58	41	12	7		4 (Agree)
	Percent	49.2	34.7	10.2	5.9		

The action officers, records staff and records managers were furthermore asked to explain the effectiveness of existing e-records management policies, guidelines, and regulations. All 118 (100%) concurred they were inadequate.

The study sought to find out whether Moi University has any international standards that are adhered to in achieving e-records security (Appendix 3 question 3). The results showed that 10 (62.5%) of the respondents mentioned quality management system and procedures that are derived from the ISO standard 9001:2015, while 6 (37.5%) reported that there was no standard in e-records security management. The responses were summarised in the words of two respondents R6 and R7 as follows:

> R6: *"This is a professional area which few people within the university will understand some standards guide e-records security management from creation to disposal. Moi University does not apply these standards. Records management is a specialized area, and in the absence of a university-wide records manager, it is not possible to establish a functional record management programme that ensures that information and e-records generated are maintained. In the absence of such a programme, it is difficult to ensure that best practice standards are followed. One needs to have a well-structured Records Management Office with adequate and proper infrastructure, trained personnel who will understand the best practices in the management of these e-records. However, it does not mean that Moi University does not maintain records, the university manages records as a stand-alone activity through registries, and the registries have people who are trained in records management. However, overall, the university lacks a proper guideline that streamlines e-records management. On the issue of standards programme, ISO 15489, MoReq, and DoD are among standards that guide the management of e-records and security and ensure that proper practices are maintained. However, the university does not practice any of them. In the absence of a well-structured records management programme, it is difficult to achieve sound e-records security management and e-records management."*

R7 stated:

> *"We are in the process of coming up and implementing information security standard based on the ISO/IEC 27001:2013 which focuses on information security. We have done some sensitization, briefed the management, deans, and schools. Therefore, it is a continuous process. In the next financial year, we are considering the issue of certification of the standards to allow its implementation in the university. This is a wider requirement from the Ministry of ICT. The Ministry has asked all the universities to implement that*

> *standard as a measure to secure information as information is an important asset of the university."*

The study sought to establish how e-records affect the implementation of ISO 9001:2008 at Moi University (Appendix 2 question 22). All the 5 respondents reported that ISO 9001:2008 advocates for documentation as evidence of activities carried out and that during audits by ISO represented by KEBS, mostly hard copy records are used as evidence for the activities carried out which lead to the creation of many paper records. The respondents further brought to the attention of the researcher that the University is in the process of implementing ISO 9001:2015, which advocates for the electronic form of information and services. The responses are summarised in the words of R2 that:

> "*Part of the ISO certification that we implemented in 2015 espouses electronic form. From 2008, there was much creation of records and most of it was in hard form, and the storage was a problem. However, with time as ISO 9001:2015 advocated for records to be in electronic form, we are going to ensure that records are available and accessible in this format. We are anticipating that the impact will be positive for efficiency regarding retrieval and storage and having a cleaner environment."*

5.5.1.3 Extent the University vision, mission or strategic plan encapsulated e-records management

The study also sought to identify the extent the University vision and mission encapsulated e-records management (Appendix 1 question 9; appendix 2 question 3). From the interview findings, 3 (60%) indicated that they were not aware of the university's vision and mission encapsulating e-records management, 2 (40%) were of the opinion that the university vision and mission is to see all services and activities automated to enhance efficiency and effective service delivery.

> One of the respondent (R21) quoting the universities vision stated that the University vision is nurturing innovation and talent in science and technology and development; thus e-records should be one of their area of investment, but that is not the case.

Responses from questionnaires indicated that 43 (36.4%) of respondents were not aware of the extent to which e-records management is encapsulated in the vision, mission or strategic plan of Moi University, 44 (37.3%) indicated that e-records was not at all encapsulated in the vision, mission or strategic plan of Moi University, 22 (18.6%) indicated that university vision and mission encapsulated e-records management to a less extent while 9 (76%) indicated that records management is encapsulated in the vision, mission or strategic plan of the university to a great extent as shown in figure 14.

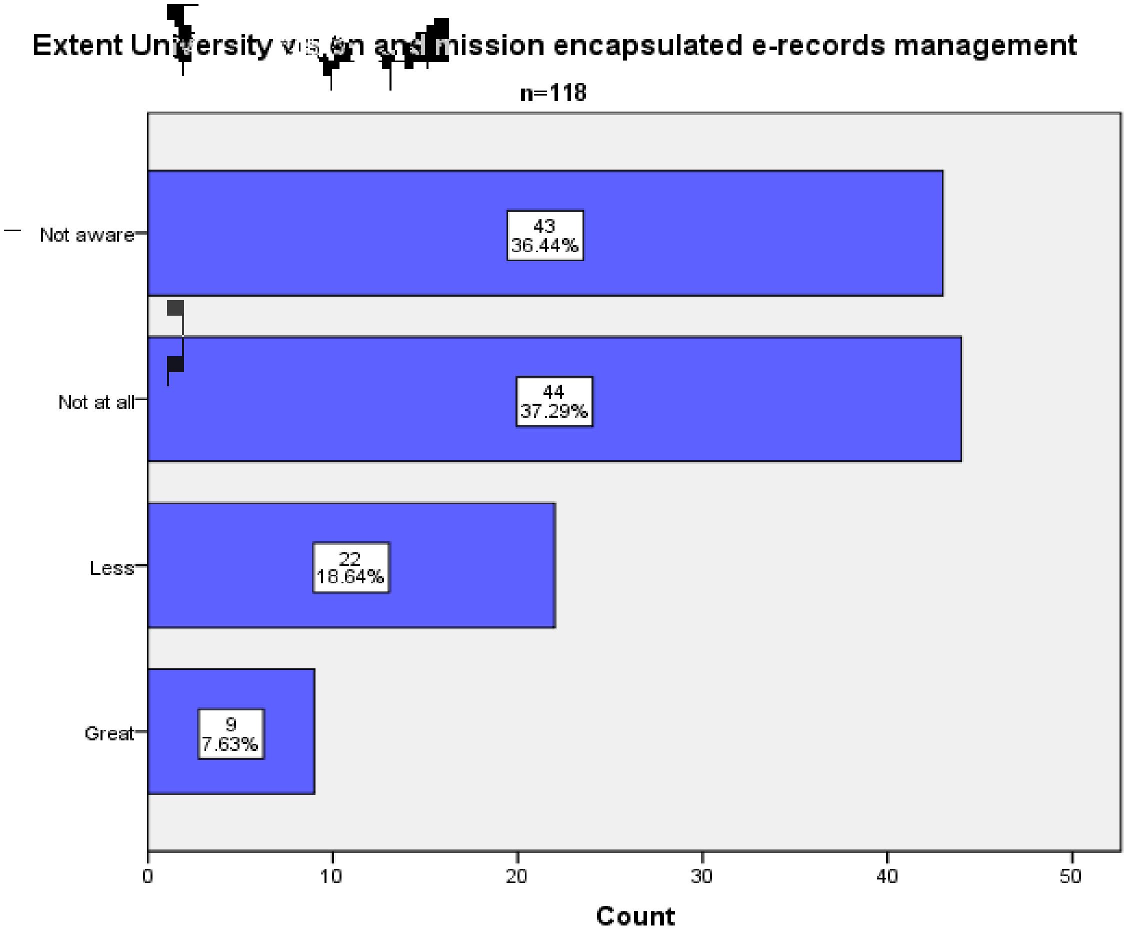


Figure 14: E-records management encapsulation in the vision, mission or strategic plan (n=118)

5.5.2 Security classification of e-records process handling to facilitate description, control, disposal and access

The other objective of the study was to investigate the security classification of e-records process handling to facilitate description, control, disposal, and access. To understand this research question, the researcher asked several questions (Appendix 2 questions 7-17; appendix 3 questions 6-13; appendix 1 questions 12-15). Several questions were posed to respondents through interviews and questionnaire to reach the objective.

5.5.2.1 Practices that affect the security of e-records management at Moi University

The respondents were asked whether they are aware of how e-records security is practiced and managed. Data from the interviews showed that all 21 (100%) said that, the e-records security management is decentralised and done without any guidelines, but staff uses their knowledge and skills to ensure the security of their e-records. They noted that each department or school have their way of carrying out e-records security management. Respondents (R7, R6) had this to say:

R7: stated:

> *"Issues of security is a responsibility of everyone and are very pertinent. It is more of management function than technical function and responsibility to everyone where each person has to play and also the other users who have to put in their security measures, thus, we normally try to improve every time."*

R6: observed:

> "*Officially, Moi University does not have a well-defined records management system per-se, but they have functionalities that are electronic for example, finance, and examinations, accommodation. No guidelines or manuals are setting out the fundamental issues in e-records security practices. However, we have minimal practices to secure e-records."*

The respondents went ahead to mention practices in e-records security in Moi University as follows:

"Allocation of access right depends on your role and your mandate."

"Use of passwords,"

"Information accessed by authorised personnel."

"Updating software and hardware and regular maintenance of computers servers storing information on emails."

"Backing up on cloud computing (google drives), external disk and other storage devices."

"Having security personnel roaming around and inside the building."

"Having burglarproof doors and grills on windows."

To understand more on the e-records security issue, the respondents were asked whether the e-records security management component is included in the organisation structure of the university (appendix 2 question 6). All the five (5) top management respondents reported that e-records security was represented through ICT directorate, which is represented on the organisational structure. The responses are summed in the responses of R1:

Respondent R1 reiterated that:

> *"ICT directorate guides the functions of ICT including information in electronic format, by representing, tabling, suggesting and advising the university on ICT infrastructure, including internet and intranet connectivity and bandwidth."*

The respondents were further asked to state the University's security plans for the next 5 years. The responses were as follows:

> *"Giving more financial support to ICT as it is an essential tool in e-records and economic development of the country in that it enhances service delivery, communication, access to business opportunities and allows communities to engage in the knowledge-based economy of the 21st century. Kenya's vision 2030 positions ICT as a foundation for penetrating the knowledge economy and so Moi University is awake to the opportunities and possibilities presented by ICT. It is envisaged that the university will achieve higher levels of service delivery through ICT optimisation and greater customer satisfaction. In aligning itself towards achieving vision 2030, the University aims at integrating ICT in all its services."*
>
> *"Achieving a fully integrated information management system that will incorporate most of the university activities."*
>
> *"Continuous backup of information on servers and other storage devices."*
>
> "*To ensure that all function and activities are highly automated*
>
> *"Digitisation of paper records and storing in accepted designated storage devices or systems."*
>
> *"To ensure Procurement plans are implemented yearly thus new, and upgraded software and hardware are carried out annually."*

The respondents were asked whether e-records security management is subject to any external audit (appendix 3 question 7). The results revealed that 12 (75%) were of the opinion that there were no external audits carried out, while 4 (25%) reported that e-records security management is not directly subjected to external audit, but whenever KEBS come for the ISO audit, they ask for documentation and sometimes if communication was via email or soft copy they request to be shown the email or the e-record. Some of the responses are summarised in the words of R7, R6:

> R7: *"The external audits are carried out, for example, last year (2017) KPMG conducted an external audit on financial management systems and hostel management system in the university on e-records among other areas."*

R6: Contrary opinion was that:

> *"Audit is complicated in Moi University. Who is responsible for e-records management? In the absence of that person, it is difficult to ensure that records in the first place are being managed. When it comes to e-records, there is no harmonisation approach to this, and the issue is neither here nor there. There is no audit on e-records security management. Many countries strive to establish what we may call best practice guideline, for example, the Australian guideline on e-records 2004. With this, then institutions can come up with customised procedures; unfortunately, Moi University does not have."*

On the availability of infrastructure to support e-records security management (appendix 2 question 10), all the five (5) top management respondents provided the following responses:

> *"Hardware (computers, server's backup generators UPS, firewalls."*
> *"Network security (firewalls and antiviruses)"*
> *"Internet services provided by Kenet and Safaricom."*
> *"Internal bandwidth and Wi-Fi located at specific Hotpoint for example library, administration block, and all schools."*
> *"Human resources which help in manning, maintenance and operations of ICT equipment. They report to the dean of respective school and director of ICT."*

Further, the study sought from the respondents (Appendix 2, question 9 and appendix 3 question 9) to state the adequacy and comprehensiveness of a budget for e-records security management. The results indicated that 18 (85.7%) believed there was no budget for e-records security management, 3 (14.3%) said there was some money allocated but meager, which is a significant concern. The responses have been summed up in the words of R7, R10, and R17 respectively.

> R7*: "Some money is allocated to general activities of ICT and security. This amount does not go into e-records management. The funds are not adequate, but it is just minimum to carry out few activities and basic operations. In most cases, we get additional funds from development partners through projects which we use to buy equipment."*

R10: noted:

"Most of the equipment's for example laptops and external storage devices are personal. Most schools receive computers from donations, and running a number of projects in schools assist us to get the computers. The school also consolidates its limited finances and purchases computers."

R 17 observed:

“There is a budget for the general running of school activities, but not none for management of e-records. However, for equipment, we do not procure directly we capture them on the procurement plan then the university can allocate money and buy for us, which also in most cases does not happen.”

Likert scale items were used to measure the respondents' attitude towards e-records practices. Responses from the questionnaires computed on median statistics indicated that 14 (11.9%) strongly disagreed with the e-records practices, 43 (36.4%) disagreed with the e-records practices, 30 (25.4%) were undecided, 26 (22%) agreed and only 5 (4.2%) strongly agreed, with e-records practices as shown in figure 15.

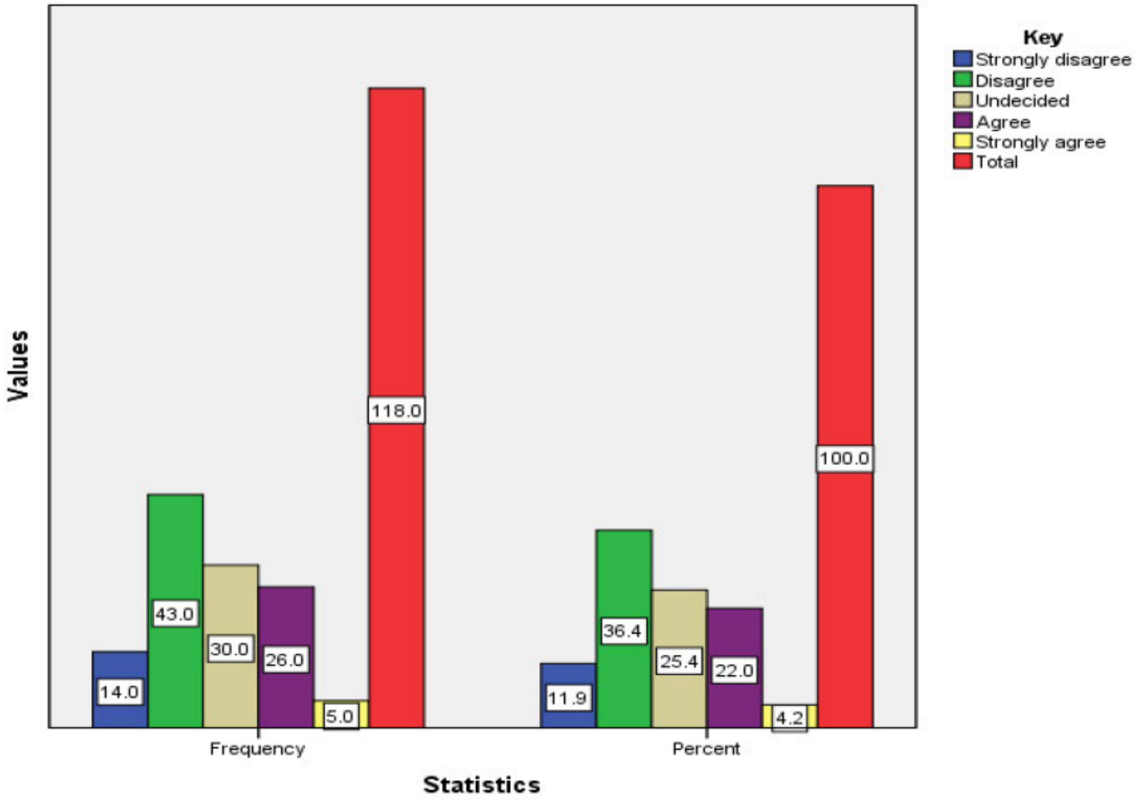


Figure 15: Attitude about e-records practices (n=118)

Specific analysis of the assertions about e-records practices is summarised in table 22.

Table 22: Attitude about e-records practices (n=118)

Assertions		**Strongly disagree**	**Disagree**	**Undecided**	**Agree**	**Strongly agree**	**Mean**
The University's e-records security practices make it stand out among other institutions	Frequency	49	48	9	6	6	2 (Strongly disagree)
	Percent%	41.5	40.7	7.6	5.1	5.1	
Availability of adequate policies and regulations framework support	Frequency	45	55	7	5	6	2 (Disagree)
	Percent%	38.1	46.6	5.9	4.2	5.1	

Assertions		Strongly disagree	Disagree	Undecided	Agree	Strongly agree	Mean
sound e-records security							
The University's achievements in its operations can be attributed to its e-records security practices	Frequency	30	34	12	19	23	3 (Undecided)
	Percent%	25.4	28.8	10.2	16.1	19.5	
The threat management and assessment carried out in the university is attributed to the security of records in the university	Frequency	8	5	16	49	40	4 (Agree)
	Percent%	6.8	4.2	13.6	41.5	33.9	
The access control mechanisms and safekeeping of passwords have enhanced the security of e-records	Frequency	8	9	18	52	31	4 (Strongly agree)
	Percent%	6.8	7.6	15.3	44.1	26.3	

Further, the action officers, records managers, and records staff were asked to indicate the e-records security initiatives available. The findings indicated that E-records security and training programmes and e-records security management policy were the most available at 118 (100%) and 117 (99.2%) cases constituting 21% and 20.9% respectively. The rest of the multiple response result is presented in table 23.

Table 23: e-records security initiatives available at Moi University (n=118)

		Responses		Percent of
		N	Percent	Cases
Security initiatives	E-records security and training programmes.	117	20.9%	99.2%
	Frequent backing up of e-records.	42	7.5%	35.6%
	Threat management and assessment programmes.	93	16.6%	78.8%
	Security and access classification of e-record for instance, top secret, sensitive, classified, confidential.	82	14.6%	69.5%
	E-records security management policy.	118	21.0%	100.0%
	Monitoring and auditing e-records protocol.	82	14.6%	69.5%
	Physical control and monitoring of the workplace environment and computing facilities.	27	4.8%	22.9%
Total		561	100.0%	475.4%

a. Dichotomy group tabulated at value 1.

The respondents were further asked how self-evaluation and review on security practices is done (Appendix 3 question 8). The results revealed that 13 (81.3%) respondents reported that self-evaluation and review on e-records management is not done, while 3(18.7%) reported that it is done; however, those who said it is done indicated self-evaluation is done on service and ICT process. The responses are summarised in the words of two respondents (R12, R6, respectively).

R12 noted that:

> *"We do self-evaluation and review. The feedback we receive either from students, other clients and staff guides this evaluation."*

R6 observed:

> *"Periodically we normally audit our e-records if they maintain integrity, we know who has been accessing our records by looking at the audit trails and access logs."*

The same question was directed to action officers, records managers, and records staff. The results showed that majority of respondents 72 (61.0%) indicated they never carry out self-evaluation and review of e-records security management practices, 24(20.3%) said they do that annually, while 22(18.6%) indicated once per semester as shown in table 24.

Table 24: Frequency of self-evaluation (n=118)

		Count(n=118)	Percentage %
Valid	Once per semester	22	18.6%
	Annually	24	20.3%
	Never	72	61.0%
	Total	118	100.0%

5.5.2.2 Security classification of e-records and access controls

To understand security classification, the respondents were asked the roles they played in business activity analysis of the University (Appendix 3 question 10). All the 16 (deans and directors) noted that they are involved in the business activity analysis where their roles include but are not limited to, tabling, deliberating, discussing, giving suggestions and recommendations and making decisions on the university business processes, which are assigned to their specific offices (referring to those earlier highlighted in section 5.5). For instance, 14(87.5%) reported that they are involved in business activity analysis at school level, university senate level and deans committee level and externally areas of academic matters, financial, planning and administration, student affairs, staff matters, outreach, research, community services among others. Other 2 (12.5%) (Directors) were also involved in business activity analysis as their counterparts to fulfill the requirements of their directorates as indicated in section 5.5 that of quality control matters including teaching process and other university services, project planning, implementing ICT activity processes. The responses are summarised in the words of respondents R13 and R7 respectively.

R13 stated that:

> *"Besides academic, research, teaching, we represent the school at all university meetings for instance Senate, deans' meetings where we discuss and deliberate on matters affecting the university and come up with suggestions and solutions to enable decision making. We also have different departments in the school, and each department has a business unit. Every month we have a school management board meeting where we get updates from colleagues, and within the departments themselves they also hold meetings and deliberate on the areas of improvement, which are later tabled at the level of deans, committee of Senate and committees' of the university."*

R7 noted that:

> *"We are involved in the business activity analysis to some extent because of the information we host and the insights and direction we provide on ICT infrastructure and processes, we provide an ICT plan, give ideas, on the same at both deans committee or at school level and Senate level. Also, we receive suggestions from different stakeholders of the university on issues of computers, bandwidth, and internet coverage among others."*

The respondents (appendix 2 question 15) were asked how business activities are aligned to access classification. The results showed that 3 (60%) of the respondents believed it is difficult to align access classification because of the lack of proper guidelines. Another 2(40%) indicated that business activities are aligned to access classification. The responses were summed up by the respondent (R3) and (R4) respectively:

Respondent R3 said that:

> *"Access classification is controlled by individual departments for example purchasing, finance, and examination you cannot change anything only the department who has custody can make changes. Specific section heads and units manage the different software used for example examination, library, and finance."*

Contrary opinion of respondent R4 indicated that:

> *"With the inadequate implementation of the available legislation and lack of guidelines, it is difficult to have a procedural and systematic alignment of records classification to the business process."*

Further, the researcher probed whether the university classified its e-records, 21 (100%) respondents noted there is some security classification that is applied. Though majority 19 (90.4%) of the respondents indicated that there was no clear guideline and direction on the same, but depending on the business function, security classification was applied, while 2 (8.6%) indicated, there were guidelines on the same referring to the quality manual procedures. ‘Confidential', which was being applied to personnel records, student records, medical records, and legal records’; ‘Top secret' was applied to records created or passed through or could be accessed by minimal number of users including e-records from deliberation of the University Council, fiscal records, students examinations among others; ‘public' those accessed by both members of staff and the community including notice of upcoming events that is sports, request for tenders, medical campaign, rallies, walks, job advertisements among others; ‘internal use' which are meant for day to day university personnel and students including notice of meeting for either staff or students, university policy documents, service charters, performance contract records, internal job advert notices, notices for internal upcoming events, among others. The responses were summed up in the words of (R6):

> *"That the university lacks a written e-records classification scheme, which could have helped in providing an organised way of classification and provision of restrictions applicable to e-records. While that being the dilemma, classification of activities by departments, schools and other units is done in relation to the nature of the activity in most cases.”*

The respondents were also asked on how security classification of the e-records process is handled to enhance access control. The results showed that 21 (100%) said that description, control, link and determination of disposal and access status is done by respondents in diverse ways. Five (23.8%) indicated that e-records created and or received at top management level are described and linked to the function that leads to their creation; thus, determining access status which is that of nature of the business activity, role played and individual's rank. For example, those records from university council are not accessed by anyone, but those with privilege to access is determined with their role and rank. The respondents unanimously indicated that determination of the disposal of records is not generalised, but records are given longer access periods. Sixteen (76.2%) shared the same sentiment that a role and level of or position of a person determine access to certain types of e-records for example, a school administrator maintains access to student marks at the school level and at the departmental level, the department head. The respondents indicated that disposal is rather complicated, because e-records are not disposed.

The responses are summarised in words of respondents R7 and R13 respectively.

R7 said:

> *"We have a number of controls regarding access to ICT and different levels of security. We have different principles we use, for example, the Principle of least access whereby one is required to access information that they need not everything in the database. An administrator is allowed to access information that is relevant to her/his work, but she/he cannot go for example to check on health records, salaries, or financial information on the systems. Somebody like the Vice Chancellor can have more access rights than someone at the middle level and lower level. Each user has a privilege that only allows access to what one requires. Not all users are allowed to delete anything, an ordinary user cannot delete a record, a record cannot be deleted by one person, but cascaded and deleted by the head of the department that is if deletion is an option; the deletion goes through stages, there are stages before a record is deleted, but the person who can delete is the person who has a super user or administrative privileges or higher privileges. If an ordinary person who has fewer privileges marks a record for deletion, the deletion process is cascaded upward."*

R13 observed:

> *"After creation, records are named in relation to the business activity that led to their creation. E-records are stored in internal computer drives, email, external hard drives, compact disks, in order to ensure the protection of vital information stored, these storage*

> *devices are fitted with powerful, unique passwords, and encryption to deter unauthorised access, and security storage media are kept in rooms fitted with grills and CCTV camera to monitor any movements. Access is only granted to authorised staff; Offices are fitted with firefighting equipment such as fire extinguishers and hose pipes."*

Responses from questionnaires on whether the respondents were aware of e-records security classification and level of access indicated that 63 (53.4%) noted they are not aware, while 55 (46.6%) specified that they are aware of security classification and level of access at Moi University. Those who said security classification was available were further asked what security classification was available. Out of the 46% of the respondents who indicated to be aware of security classification and level of access, 27(22.9%) specified internal classification level, 13 (11.0%) stated public, 10 (8.5%) itemised confidential and 5 (4.2%) identified secret classification level, while 63 (53.4%) were not able to give a response.

On whether they were aware of the existence of access policy and what it entails; responses from interviews revealed that all 21 (100%) respondents concurred that there was no access policy. However, the respondents mentioned Quality Management Procedures (QMP) and the ICT policy as the available tools. When asked whether they knew what they entail, they responded that the QMP defines the roles of every individual and assigned duties depending on their category. Respondents were further asked if available policies imposed security classification or any other restrictions. The results showed that 21(100%) of the respondents indicated that classification of each of the information was done in relation to business processes of the university because it was not well documented; thus, security classification is neither here nor there. For instance, information which should have some limited access, and those that have least privileges are determined by each department in relation to the business process.

Moreover, responses from questionnaires indicated that 109 (92.3%) of the respondents generally indicated that there was no e-records security classification policies or guidelines and 9 (7.6%) indicating ICT policy as a guideline.

The study wanted to find out whether the university has a user permission register and how it distinguishes the privileges of users (Appendix 2 question 14). All the 5 top management respondents stated that there is no written user permission register, but user permissions are based on one's level in the university structure, the roles played and privileges accorded to individuals.

5.5.3 Security threats to e-records

The study sought to find out the security threats predisposing e-records to damage, destruction or misuse (appendix 1 question 17-22, appendix 2 questions 18, 19 appendix 3 question 14). In this regard the researcher sought to know whether the university carries out a threat assessment. The 5 (100%) top management respondent indicated that threat assessment in the university was achieved through both internal and external audits on the university business process and that during the process the auditors identify threats to e-records. The respondents' views on issues that guide threat assessment expressed different opinions as follows:

> *" New technologies and their challenges."*
>
> *" Documentation about hardware and software."*
>
> *" Reports from both internal and external audits."*
>
> *" Information about network connectivity."*
>
> *" Self –evaluation, monitoring and through a performance contract."*
>
> *" Quality assurance reports."*
>
> *" Document that describes available systems, system functions and boundaries information about university vital records."*

The responses are summed up in the words of respondent (R5) that:

> *"The most known threat assessment practice is the internal and external audits. During auditing of the university business activities by both auditors from KEBS, KPMG, and the internal university auditors, security threats may be identified, and I also assume ICT department carry out a threat assessment on the ICT infrastructure."*

Moreover, the action officers, records staff and records managers were asked to state whether the university carries out threat assessment. The results showed that 63 (53.4%) indicated the university never carry out a threat assessment program, 8 (6.8%) reported that a threat assessment program is carried out twice per semester. Detailed responses are summarised in table 25.

Table 25: Threat assessment (n=118)

		Count(n=118)	Percentage %
How often does the University carry out threat assessment program	Never	63	53.4%
	Once per semester	18	15.3%
	Twice per semester	8	6.8%
	Annually	15	12.7%
	Biannually	14	11.9%
	Total	118	100.0%

The respondents were further asked the e-records management threats that the university faces. The majority of the respondents who were interviewed indicated lack of policies and lack of implementation of regulatory frameworks, inadequate qualified and trained personnel, cyber-attacks, staff collusion, leaking and theft of information, mishandling of hardware and storage devices, a highly networked environment which compromises security, computer theft, and lack of training programmes. The responses are further summarised in the words of two respondents (R12, R20) respectively:

R12 indicated that:

"We are in a very porous environment where students and staff walk in and out of offices with sometimes little or non-monitoring. This has led to a number of laptop theft and attempted break-in offices. This has happened despite having security guards. In other cases, an office can be closed after working hours which is at 5 pm but the following morning one would hear complaints that a computer had been stolen, which leads to the conclusion that it is an 'inside job' and or collusion with students who are on campus almost all the time."

R20 respondent explained that

"Cyberspace has led to increased challenges which organisations like Moi neither anticipated nor had made plans to prevent. Cybercrime and network threats that are all over the internet have brought with it a great number of challenges. This includes virus attacks, denial of service where a document or computer is corrupted among others."

R6 explained that:

> *"The e-records are captured and held on a computer; when it comes to long-term preservation, it is a difficult thing. The university depends on the stand-alone servers to capture and maintain and either preserve records, and it is doubtful whether they do it. The lack of a central server is an issue. When the computers are 'old,' and they need to be retired, there is no much attention given to e-records. E-records are new and more challenging and complicated, and there is no expertise to help preserve e-records to posterity. One will expect ICT will help, but they only deal with tools and software, internet and ensuring computers work, so e-records is a different ball game. The e-records are vulnerable. How they are captured, maintained, who is responsible and how long they should be maintained and what policies and standard should be used is a significant problem at Moi University."*

The records staff, action officers and records managers were also asked a similar question. The question drew open-ended responses, which were analysed categorically with 95 (23.5%) citing cybercrime threats, 106 (26.2%) cited employee error threats, 103 (25.5%) indicated technological threats and 100 (24.8%) were classified as others as presented in table 26.

Table 26: E-records threats on security threats (n=118)

		Items	**Count (n)**	**Percentage%**
Valid	Cyber crimes	Hackers and crackers, Attacks from viruses	95	23.5%
	Employee threats/errors	Mishandling, Loss, and destruction of data, Lack of management, Unqualified and untrained personnel, Too much IT access for employees, Internal employee threats	106	26.2%

	Technological	Poor storage of computers/machines, outdated computers, backup mistakes, Damaged computers	103	25.5%
	Others	Lack of storage spaces, Environmental hazards, Lack of enough funding to purchase computers, lost /stolen laptops,	100	24.8%
Total			**404**	**100%**

Along the same line but with the intention to find out specific threats on the preservation process of e-records, the study listed likely threats. Hackers and crackers were identified by 22 (6.7%) respondents, attacks from viruses reported by 26 (7.9%), environmental conditions came in at 33 (10.0%), technological obsolescence by 65 (19.8%), loss and destruction of records was reported by 87 (26.4%), while mishandling was reported by 96 (29.2%) respectively. These results are presented in Table 27.

Table 27: Specific threats on preservation process of e-records (n=118)

		Responses		
		N	Percent	Percent of Cases
Multiple	Hackers and crackers	22	6.7%	18.6%
	Attacks from viruses	26	7.9%	22.0%
	Environmental conditions	33	10.0%	28.0%
	Technological obsolescence	65	19.8%	55.1%
	Loss and destruction of records	87	26.4%	73.7%
	Mishandling of e-records	96	29.2%	81.4%
Total		329	100.0%	278.8%

a. Dichotomy group tabulated at value 1.

The respondents were further asked the strategies that are used to overcome the preservation challenges they experienced. They reported as follows: staff capacity building 47 (39.8%), computer security plans 38 (32.2%), and backup recovery 33 (28%) as shown in figure 16.

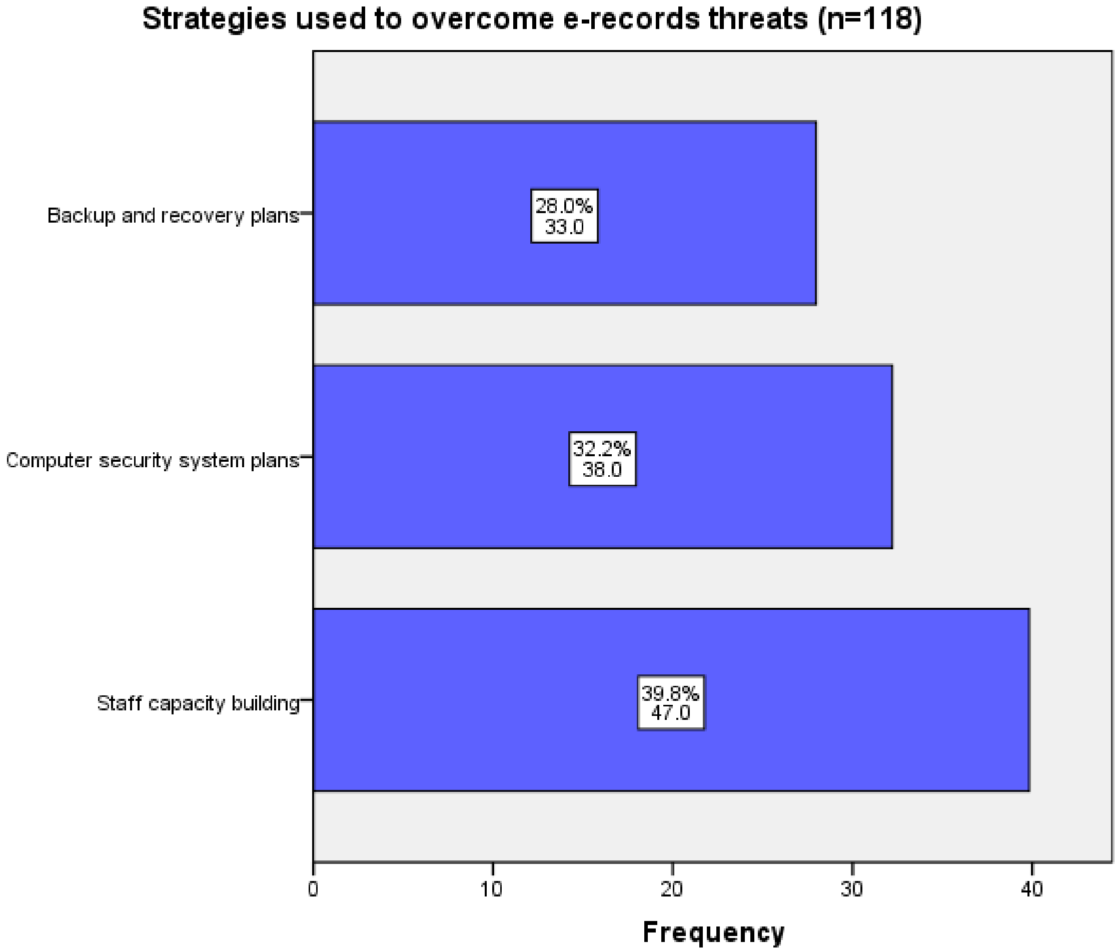


Figure 16: Strategies used to overcome e-records threats (n=118)

The study further sought to identify possible solutions to the security threats identified above. Those interviewed advocated for the urgent development of policies, programmes and implementation of the regulatory framework, capacity building and continuous education and training, monitoring and evaluating systems, protecting networks against cyber-attacks, frequent backing up of records, strict use of access controls, having both physical and logical controls.

Moreover, respondents were asked to state critical success factors in e-records security management at Moi University. Data from questionnaires indicated that 26 (22.0%) of respondents indicated developing of information systems, 23(19.5%) indicated improved staff performance, 36 (30.5%) suggested restriction on access and sharing of information, 11 (9.3%) indicated staff training, while 22 (18.6%) indicated support from top management as shown in table 28.

Table 28: Critical success factors in e-records security management (n=118)

		Count(n)	Percentage %
Valid	Developing information systems	26	22.0%
	Improved staff performance	23	19.5%
	Access and Sharing of information have been made easier	36	30.5%
	Staff training	11	9.3%
	Support from Top management	22	18.6%
	Total	**118**	**100.0%**

5.5.4 Measures to protect unauthorised access to e-records

The fourth research question was to inquire about measures available to protect unauthorised access to records. To understand this objective some questions were asked (appendix 2 question 20-25; appendix 3 questions15-17; appendix 1 questions 22-26). To address this question, a number of areas were to be established including a set of responsibilities and practices that are exercised to protect records from unauthorised access, measures available to protect intranet against external and internal cyber-attacks, what back up measures are available to ensure the security of e-records among others.

From those interviewed, 21 (100%) of the respondents indicated that there are various measures that each department or school defines to protect records from unauthorised access. The responsibility of each department or school is to reserve the right to limit, restrict, and remove or extend access privileges to the user. Logical controls were widely mentioned including the use of passwords, PIN and digital signatures. The respondents further indicated that most of the technical security measures are handled by the ICT staff who distribute them to different schools and different departments. Other responses mentioned are as follows:

> *"Network intrusion detector and the principle of least privilege where we have many levels of access controls, you cannot access if you do not have a username and a password. To protect access from outsiders, we have put firewalls to stop intrusions."*
>
> *"Ensure the information that is entered is correct, accurate and has no errors."*
>
> *"To ensure that every level of information access is secure."*
>
> *"Records are created and managed in folders as per the activity that leads to their existence."*
>
> *"Access restriction."*
>
> *"Software and hardware maintenance and updating."*
>
> *"Back up in both hard and soft copies."*
>
> *"Access restrictions to computers and offices to authorised Personnel, to emphasize, we have physical controls at the hardware level, few authorised personnel access the servers and the place is under key and lock.*
>
> *"Continuous assessment on the network, we have a periodical network weekly assessment, we check through the access logs to see who was trying to access and if they were blocked."*

The action officers, records managers, and records staff were also asked to state the measures that are available to protect e-records. The responses revealed firewalls and antivirus protection to be most popular (57, 48.3%), followed by monitoring of internet activities at 32 (27.1%), backup and recovery and regular change of passwords strategies at 14 (11.9%) and only 1 (.8%) of respondents cited software and hardware updates as shown in figure 17.

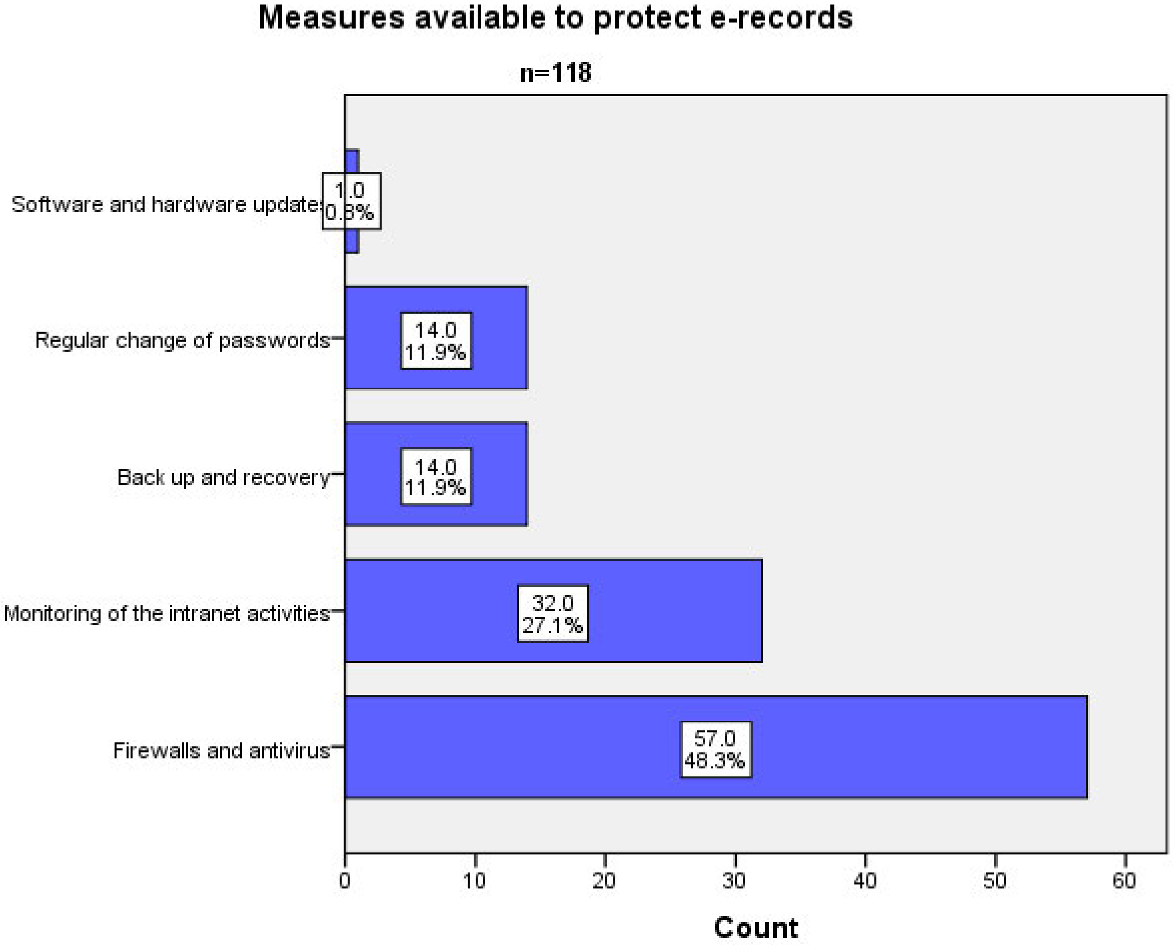


Figure 17: Measures available to protect e-records (n=118)

Regarding storage, a significant number (42, 35.6%) of respondents indicated that they stored and handled e-records in a manner that protects them from unauthorised access, loss, destruction, theft, and disaster through computer security system plans. The computer security plans mentioned by respondents included; restricted access to computers through passwords, restricted access to servers, secure student portals, minimised risk of unauthorised alteration or erasure of electronic records. Another 34 (28.8%) of the respondents mentioned backup and recovery plans (external backup drives stored in remote locations); 22(18.6%) singled out authorised usage and access (lockable file cabinets, physical security of the premises). Others at 20 (16.9%) mentioned training of personnel on how to safe-guard sensitive or classified electronic records and compliance with requirements as shown in figure 18.

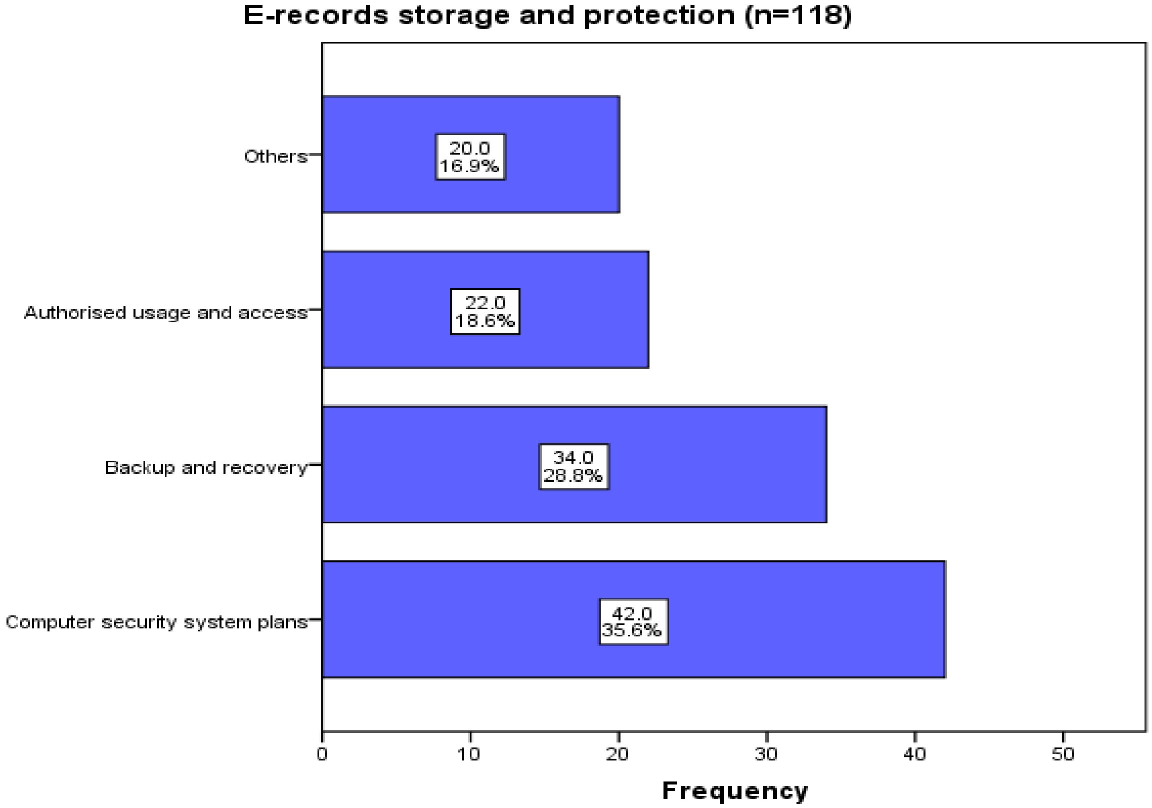


Figure 18: E-records storage and protection (n=118)

The study also sought to find out the state of physical security infrastructure available to protect e-records**.** All the 5 top management staff interviewed reported that there are security personnel in every department and all sections of the university compound and the infrastructure that habilitates e-records is secure and well maintained; also, use of burglarproof doors and grill windows is applied, and accessibility is restricted by key and lock. Responses are summarised in words of respondent R1:

> R1: *"the university has put in place a police post, tightened security personnel, and we have introduced security checks at key entry points of the buildings and gates. We also sensitise staff and students on issues of security".*

Data from questionnaires showed 22 (18.6) devices are labeled, 22 (18.6%) security guards are available, 17 (14.4%) burglar proof doors and grills on windows provided, 16 (13.6%) computer security system plans provided, 28 (23.7%) distress alarms and sirens provided, 13 (11.0%) indicated controlled access to premises as ways of enhancing physical security of the premises, ICT infrastructure, computers and laptops as shown in table 29.

Table 29: Physical security of the premises (n=118)

		Count (n)	Column %
Valid	Devices are marked	22	18.6%
	Security guards	22	18.6%
	Burglar proof grills, doors and windows	17	14.4%
	Controlled access to premises	16	13.6%
	Computer security system plans	28	23.7%
	Distress alarms and siren	13	11.0%
	Total	**118**	**100.0%**

5.5.4.1 Measures to protect intranet against external and internal cyber-attacks

The study sought to establish measures available to protect intranet against external and internal cyber-attacks (Appendix 2 question 22). All 5 respondents reported that firewalls, intrusion detection, and monitoring, hack-proof network system are in place, antiviruses and uses of passwords were mostly used to protect the intranet against cyber-attacks.

Responses from actions officers, records managers, and records staff showed that firewalls and antivirus protection was popular at 57 (48.3%), followed by monitoring of internet activities at 32 (27.1%), backup and recovery and regular change of passwords strategies twinned at 14 (11.9%). Only 1 (.8%) of the respondents singled out software and hardware updates as shown in figure 19.

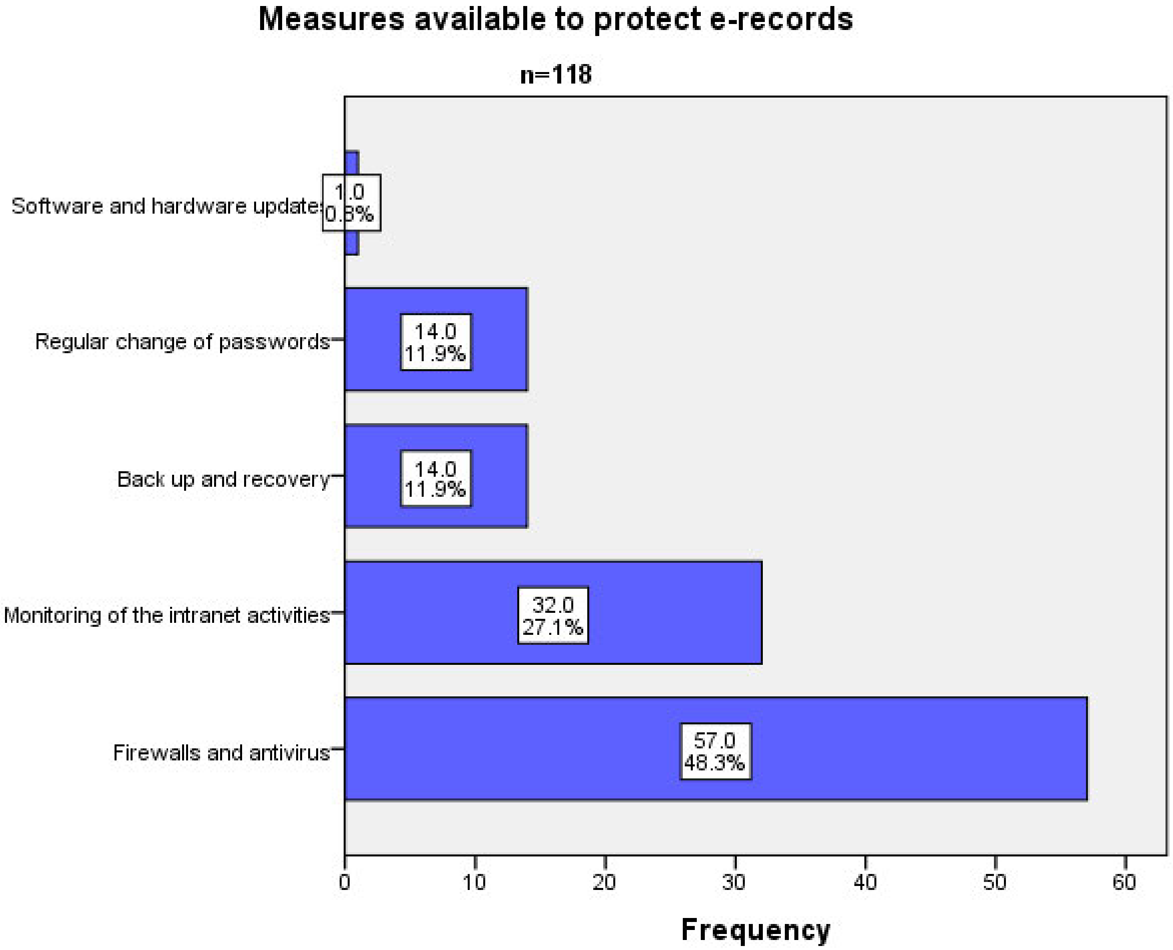


Figure 19: Measures to protect intranet against external and internal cyber-attacks (n-118)

The respondents were asked to state the backup measures in place to ensure e-records security. All 5(100%) respondents reported that the university was insured against any calamity and it had offsite storage too. The respondents further mentioned the storage of e-records on external hard drives, memory sticks, servers, use of emails and having information in different computers as back up measures.

The study also sought to find out disaster planning and recovery measures in place. All the 5(100%) respondents said that there are several measures including the physical security infrastructure discussed earlier. However, the respondent said that the university lacks a disaster management policy. The responses are summarised as follows:

> *"Carrying out fire drills by fire officers in conjunction with the fire department at the county level and national once in a while."*

> *“All the buildings have a number of fire extinguishers.”*
>
> *“The buildings are also well maintained and cleaned while some of the buildings have caretakers.”*
>
> *“The university has also ensured that an electrician is on duty to help in the event there are power issues*
>
> *"Encouraging staff members to frequently back up information."*
>
> *"Encouraging staff to store information on their official university emails."*

The study sought to find out how directorates and schools ensure quality control in the security of e-records (appendix 3 question 17). The results showed that 13 (81.3%) respondents reported that they do not carry out quality control on e-records security because of the lack of guidelines and policies. However, they rely on ICT department through their ICT staff at the school level to maintain and update software and hardware to enhance quality assurance. Another 3 (18.75%) noted that quality control is done through providing adequate bandwidth, backup generators, evaluating and checking complaints and feedback from students, staff and other stakeholders, which we use to make the adjustments where possible. The responses are further summarised in the words of two respondents (R7, R6) respectively:

> R7: “*As part of quality assurance, we make sure the services are available. We have a generator near the central server, in case of a power blackout, the information on the database or server is available and accessible. The university has also increased bandwidth, we have been improving and making sure it is sufficient to enable quick access of records that are hosted in the central databases, though it has not been sufficient we have been upgrading every year, the last upgrade was this year in January which doubled the bandwidth from 191 to 832 megabits per second.”*

R6 explained:

> *“Quality assurance on e-records security management does not happen because of lack of proper guidelines and policies. For example, generally in other universities, there is no use of personal email when transacting official university documents, but this frequently happens in the university here.”*

5.5.5 Confidentiality, Integrity, Availability, Authenticity, Control and Utility of E-Records

The research question two sought to find out the security ethical values of confidentiality, integrity, availability, authenticity, control, and utility of e-records (appendix 1 question 27; appendix 2 question 26 and appendix 3 question 18,19 respectively). The results from interviews showed 12 (57.1%) of respondents indicated that e-records security ethical values are achieved, 7 (33.3%) indicated that some of the ethical values are not achieved, and 2 (9.5%), in contrast, indicated they are not achieved. However, it is difficult to accomplish the ethical values in the university without an appropriate policy framework and necessary human resources. The university should provide proper guidelines and training guarantees for achieving confidentiality, integrity, authenticity, availability, control and utility.

. The elicited responses are summarised in the words of R7, R2,

> R7: *"This (referring to the ethical values) are vital and are some of the components that guide us on security issues. We make sure they are our guiding principles, we sensitise users on how to handle confidential, internal information among others. On issues of integrity, we store records on servers, and there is limited access to those records. Availability we make sure the network is operational, servers are working, and we know that the value of information is in its availability. Authenticity is observed to maintain the originality of the records, if it loses authenticity information loses value, we make sure original information is available, we have put many controls in place on how information is used, and accessed for example for servers only individuals with access rights can enter there, we have both physical control and administrative controls. For example, passwords are used to ensure information is secured. The information on the website is public, and we make sure the only person who can update it is the webmaster who has authority to access web servers that host the website and, who has a username and password and can make changes and replace information. Any other person cannot make any changes but can only read what is on the website."*

R2 noted:

> *"Records are created and accessed at various levels, for example, those meant for consumption by university council are accessed at that level and only accessed by*

authorised personnel at that level. Through this, integrity is observed, availability is limited to authorised personnel, and authenticity is achieved by referring to the authors at a given level who are allowed to access it. Possession is limited to those who are authorised to access the particular information depending on the nature of the information that one needs, and the e-records are given administrative rights at various levels so that some have higher rights others have low rights. The major problem is that they limit the usefulness of e-records (limiting utility). Sometimes information is needed or required urgently, and someone is not around, and no one else has the right to access the information it then becomes a major problem. For instance, when the government needs information urgently, it becomes a problem when people with specific rights are not available. This problem has widely been brought about by lack of integration of the available systems."

R9 asserted:

"Loss of laptops, IPad, mobile phones and external storage devises to thieves both on campus and outside campus which have led to the loss of vital e-records and other information. Most of the devices are not encrypted and lack passwords, which has led to compromising confidentiality, possession, and utility of the information and the devices.

The respondents went further to explain how each of the security ethical values can be achieved and the responses are summarised in table 30.

Table 30: Security ethical values (n=21)

Security ethical values	**Response**
Confidentiality	"Use of passwords and restricted access to authorised personnel."
Integrity	"Having access levels and privileges (super user, ordinary user, administrative user)" for different assignments.
Authenticity	"Different stages of approval, signatures and dated."
Availability	"Availability of the internet."

Possession/control	"Read-only privileges on the website, use of passwords, encryption, physical control, use of privileges."
Utility	"Availability of passwords and keys, access allowed to personnel with privileges."
Accessibility	"Maintaining computers, updating software and hardware, having passwords."

A Multiple response question was used to establish whether e-records security ethical values have been achieved or not achieved. The Dichotomy group tabulated at value 1 equal to “achieved” indicated that 57 (48.3%) response cases representing 19.7% of the respondents agreed that availability of e-records was achieved, 30 (25.4%) response cases representing 10.4% of the respondents agreed that Integrity of e-records was achieved. The rest of the results are summarised in table 31.

Table 31: E-records security ethical values (n=118)

		Responses		Percent of Cases
		N	Percent	
Ethical_Values[a]	Availability of e-records	57	19.7%	48.3%
	Confidentiality of e-records	46	15.9%	39.0%
	Possession/control of e-records	42	14.5%	35.6%
	Authenticity of e-records	41	14.2%	34.7%
	Utility of e-records	40	13.8%	33.9%
	Accessibility of records	33	11.4%	28.0%
	Integrity of e-records	30	10.4%	25.4%
Total		289	100.0%	244.9%

a. Dichotomy group tabulated at value 1.

5.5.5.1 Vetting of staff in meeting the ethical values

The respondents were asked whether vetting of staff is carried out (appendix 3 question 19). The results revealed that 14 (87.5%) of the respondents stated that they do not vet staff as they assume that the particular member(s) of staff have undergone the vetting process during the recruitment, while 2 (12.5%) respondents said that they carry out vetting. The responses are summarised in the words of respondents, R7, and R17 respectively:

> R7: *"We carry out internal vetting in the ICT department. This is because we have sensitive university e-records on our systems for example finance, exam, and marks. We make sure those who handle and maintain this are vetted, and their integrity is known, and also we make sure not everyone in the ICT directorate access the vital records, but only those with access rights."*

In contrast, R17 noted:

> "*No vetting is done per se, but we work with the team that we have been given, and if someone is seconded, we assume he or she have been vetted by the human resource department. We only look at the employment or posting letter and just work."*

5.5.6 Skills and competencies of records staff at Moi University

The researcher sought to determine the skills and competencies of e-records available at Moi University. To address this objective a number of questions were asked (appendix 2 questions 27, 28, 29, 30, 31, 32; Appendix 3, questions 20, 21, 22 appendix 1 questions 28, 29, 30, 31). The responses from interviews revealed that 21(100%) of respondents were of the view that records and action officers should have a diploma and above, and they should also have computer skills that include knowledge on computer operations, computer package skills and how to use android phones and their operations, and records management skills.

Moreover, the study sought to find out whether the number of records officers was adequate (appendix 2 question 28). All 5(100%) top management respondents indicated that there are adequate record officers. However, when asked whether they had qualification in records and archives management or information science related qualifications, the respondents indicated that in most cases those with academic qualification in information sciences are employed in the registry, and they are not adequate, but majority in the other departments are action officers where some have the responsibility of records staff with different academic qualifications and not necessarily information sciences and records management.

The study also sought to know how the university ensures staff retention, incentives, and succession plans are provided (appendix 2 question 30 and appendix 3 question 20). The results showed that 21 (100%) observed:

> *"We try to make sure the staff are motivated by providing a conducive working environment."*
>
> *"When it comes to job opportunities, for example promotions, we consider the staff who already are in the system."*
>
> *"There are opportunities to study, but the problem is that professional records management issues are confined at the registry level."*

The study further sought to identify the type of training policy that is available for records and action officers (Appendix 2 question 31). All 5 (100%) respondents said that there was a training policy. They noted that through the university development fund, staff are given an opportunity to further their studies, in diploma and above. However, in the last few years, the university has been having financial problems, which have led to inadequate support being provided.

Moreover, all 21(100%) respondents interviewed reported that capacity building was inadequate especially regarding continuous education and training in e-records security management because of inadequate finance and lack of policies and regulatory frameworks among others. The responses are summarised in the words of R6 and respondent R18.

R6 said that:

> *"Lack of proper guidelines, policies, records management programmes has made it difficult to maintain continuous training through workshops, seminars, public lectures among others. The school of information sciences and ICT directorate have been trying to organise workshops and trainings, but they have not been sufficient in terms of frequency because of inadequate funds and goodwill from management."*

R18 stated that:

> "*The need assessment is done through appraisal where members of staff identify the training and education gaps, but that becomes the end of it after submission to the relevant offices.*"

On the question of training programmes in e-records security management available at Moi University (Appendix 1 question 28), 95 (80.5%) of the respondents indicated no training is available. Less than 20% of the respondents reported the availability of training programmes in e-records management specified as short courses, records management, information security systems training, and training on creation, storage, retrieval, use and disposal of information as shown in table 32.

Table 32: Training programmes in e-records security management (N=118)

		Count(n=118)	Percentage %
Valid	Short courses	6	5.1%
	Creation, storage, retrieval, use and disposal of information	8	6.8%
	Records management	5	4.2%
	Information security systems training	4	3.4%
	No training	95	80.5%
	Total	**118**	**100.0%**

5.5.6.1 Awareness creation among staff on e-records security

The results obtained through the questionnaire indicated that verbal communication (70, 59.3%), workshops (38, 32.2%) and online platforms (10, 8.5%) are used to create awareness as shown in figure 20.

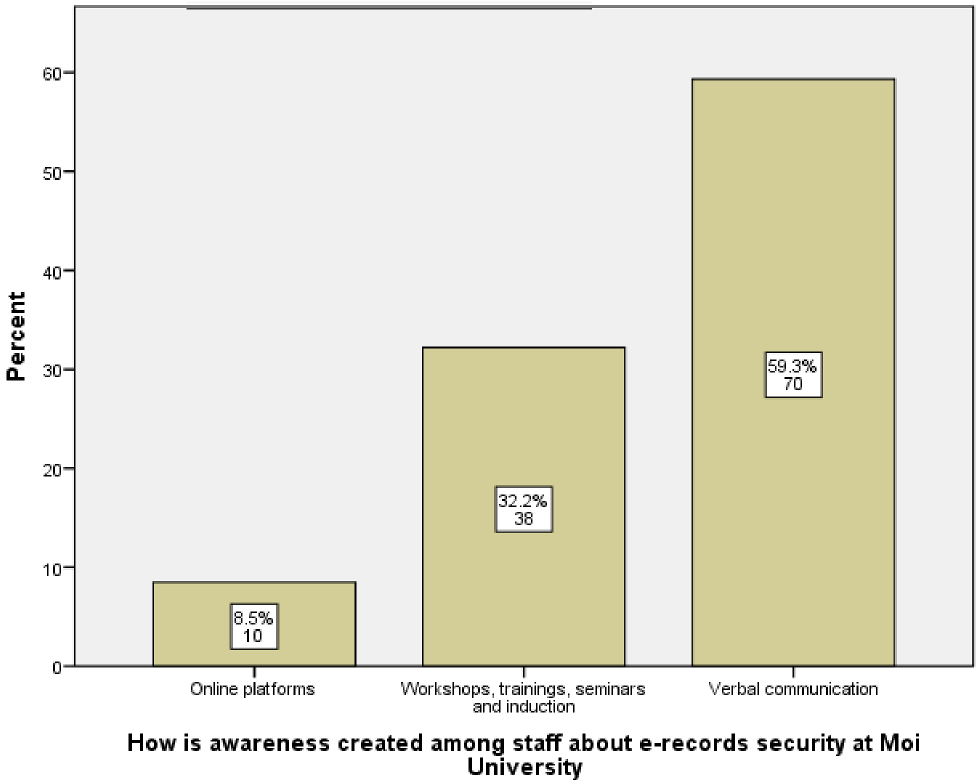


Figure 20: Awareness creation among staff about e-records security (n=118)

On the question of how often the university organises conferences, workshops/seminars and public lecturers on e-records security, the results showed that 14 (11.9%) indicated once per semester, 9 (7.6%), indicated twice per semester, 30 (25.4%) annually, 31 (26.3%) biannually, while 34 (28.8%) indicated conferences, workshops/seminars, and public lectures were never made available to staff as shown in table 33.

Table 33: Frequency of conferences, workshops/seminars and public lectures (n=118)

		Count(n=118)	Percentage %
Valid	Once per semester	14	11.9%
	Twice per semester	9	7.6%
	Annually	30	25.4%
	Biannually	31	26.3%
	Never	34	28.8%
	Total	**118**	**100.0%**

Further, respondents were asked to state whether training policy on e-records security was available. The majority of 91 (77.1%) of the respondents observed that policy for records does not exist at Moi University as shown in table 34.

Table 34: Availability of a training policy (n=118)

		Count	Percentage %
Valid	Yes - Courses on records management	16	13.6%
	Yes but not aware of the content	11	9.3%
	Not existing	91	77.1%
	Total	**118**	**100.0%**

5.6 Summary

This chapter analysed and presented the findings of the study that were collected through interviews and questionnaires under the following main themes, e-records life cycle, security classification of e-records process handling to facilitate description and access control, security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated, measures available to protect unauthorised access to e-records, how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved, skills and competencies available for e-records security management. The study findings showed that Moi university business processes have led to the creation and/ receipt of massive e-records. Majorly e-records management is decentralised with the exception of the central registry that the university manages as a standalone entity. However, the findings pointed out that the processes of e-records from creation to disposal were not well carried out. Although the processes of creation and/receipt maintenance and storage was certain, the processes of preservation, appraisal and disposal were not achieved. The findings indicated that the university lacks a records management programme and policy frameworks; thus, leading to e-records management functions being carried out unsystematically. The findings indicated that e-records security practices were undermined by among others inadequate funding, invisible e-records management and security practices on the organisational structure, weak guidelines on security classification and access controls, as well as security ethical values which were not well adhered to. The findings further indicated that the university experienced many threats that included cyber-attacks, unauthorised access, technological obsolescence, lack of storage spaces, environmental hazards, lack of enough funding to purchase computers, lost/stolen laptops and damaged computers. Regarding competencies and skills, the majority were wrongly designated. In addition, there was inadequacy of training and awareness programmes to mention a few. The next chapter discusses the findings supported by reviewed literature as well as theory.

CHAPTER SIX

INTERPRETATION OF FINDINGS OF THE STUDY

6.1 Introduction

The previous chapter presented the findings of the study. In this chapter, the researcher explains the meaning of the results presented and analysed by comparing and linking them to existing knowledge (literature reviewed) and the models applied in the study (Cell 2008; Graf 2008; Baxter, Hughes and Tight 2006).

The purpose of this study was to investigate e-records security management at Moi University. The study addressed the following research questions: How are e-records created, maintained, stored, preserved and disposed?, How is security classification of e-records process handled to facilitate description and access control?, What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated?, What measures are available to protect unauthorised access to e-records?, How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved?, What skills and competencies are available for e-records security management?. The study applied records continuum model and the Parkerian Hexad Model based on the pragmatic paradigm which advocates for the use of a mixed method. In addition, the research design adopted was a case study (single embedded case study).

This chapter covers the following subject areas: response rate, biographical profile of respondents, respondents' duties in the current position and research findings under the following themes: e-records life cycle, and security classification of e-records to facilitate description and access control; security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated; measures available to protect unauthorised access to e-records; how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records is achieved; skills and competencies available for e- records security management and summary of the chapter.

6.2 Response rate

The total number of targeted respondents were 145 (100%). Those targeted for interview were 23 (100%) out of which 21 (91.3%) were reached. Particularly, a 83.0% (5) response rate was achieved from top university management, and 16 (94.1%) were the deans of schools and directors of directorates. In addition, from questionnaires out of 122 delivered to action officers, records managers, and records staff, 118 were duly completed and returned representing a 96.7% response rate. In particular, the researcher distributed 7 questionnaires to the office of the Vice Chancellor where 6 (85.7%) were returned; 3 questionnaires were distributed to the office of the DVC academic research and extension, and all were completed and returned; 3 questionnaires were administered to the DVC finance office and all were completed and returned. The offices of the DVC administration planning and development, DVC students' affairs and the legal office each received 3, 7 and 2 questionnaires respectively. All were completed and returned giving a response rate of 100%. Moreover, five questionnaires were administered for each of the fourteen schools and all were completed and returned giving 100% response rate. The ICT Directorate and the Directorate of Quality Assurance each received 2 questionnaires, which they completed and returned. Furthermore, 23 questionnaires were administered to the Central Registry and 20 were returned giving a response rate of 87%.

Overall, the study achieved a response rate of 95.7% (139) from the survey questionnaires and interviews. The high response rate was attributed to the increased numbers of call attempts through frequent reminders and follow ups, phone calls and deliberate visits to the respondents. Furthermore, the number of respondents in the respective offices and schools surveyed were few, thus, reaching and tracking them presented a minimum challenge. Holbrook, Krosnick, Pfent (2008) and Curtin et al. (2005) assert that although in recent years there seemed to be a decline in response rate, researchers have intended to implement data collection strategies including more extended field periods, increased numbers of call attempts and sending advance letters to improve the responses.

6.3 Biographical profile of respondents

Biographical profile of respondents comprised gender, age group, level of education, duration of years worked, staff managed and scope of duties in the current portfolio. This assisted the researcher in contextualising the findings which helped in the formulation of appropriate recommendations on e-records security at Moi University. As indicated in 6.2 the respondents who completed questionnaires and those interviewed were 139 (95.7%). Of these, males were the dominating gender at 84 (60.4%), while 55 (39.6%) were female. Out of the five top management, only one was female, while of the 14 deans of schools, four were female. In Kenya, a disparity in employment opportunities between women and men remains a challenge. Consequently, a significant proportion of more men than women are employed in education, manufacturing, agricultural and social activities (Kenya National Bureau of Statistics 2017). This notwithstanding, notable improvement has been made in recent years courtesy of the spirit and provision of the new Constitution of the Republic of Kenya (2010) through the affirmative action meant to promote equal opportunities for all as we can see in the case of Moi University. On respondents age, majority (59, 50.0%) were in the age range of 20-30 years, 39 (33.1%) were in the age range of 30 - 40 years, 26 (10.2%) were between 40 - 50 years, 11 (5.1%) were between 50 - 60 years. Only 4 (1.7%) were above 60 Years. The retirement age in Kenyan Public Universities varies for the teaching and non-teaching staff as per the terms and conditions of service of each establishment. The mandatory retirement age in Kenya for non-teaching staff (action officers, records managers, records staff, legal officers, and finance officers) is 60. Particularly, those employed before 2013 retire at the age of 65, while those employed after 1st January 2013 will retire at 60 years of age. However, persons with disability retire at the age of 65 for non-teaching staff regardless of the year employed. The teaching staff (lecturers, senior lecturers, and professors) retire at the age of 70 (Moi University, Human Resource Department 2017; Kenya Retirement Authority 2011).

Regarding, level of education, majority of the respondents had the undergraduate qualification (63, 43.3%), 34 (24.5%) were Masters holders, those with PhDs were 21 (15.1%). Diploma and certificate holders were lower at 4 (2.9%) and 19 (13.7%) respectively. The introduction of parallel degree programs and burgeoning number of private universities in Kenya in the post-2000 period has seen the number of undergraduate degree holders in Kenya experience exponential growth, as such employment opportunities at the university level for non-teaching staff has given priority to those with the undergraduate level of education. This explains the high number of respondents holding the undergraduate qualification. In Kenya and other parts of the world, only a fraction of all who join graduate programme complete it (CUE Report, 2017), this corroborates the low number of persons holding PhDs and Masters qualifications at the university level. Consequently, in this study, all the deans of school and the 2 directors had PhDs which is the universities' requirement for one to be a dean (Moi University, terms of service, 2011). Most of the respondents (65, 46.8%) in the study had working experience of 3 to 6 years closely followed by 56 (40.3%) who had worked in the current position for 6 years and above while 19 (13.6%) had worked for 0 to 2 years. This result indicates a decreasing rate of hiring new employees over the years. A recent report from the university indicated that the university had frozen the hiring of new staff following an employment scandal which has bloated the workforce (The Star Newspaper 2018). As for the number of staff managed, it varied from one line manager to another for various reasons including the level and role of respondents and the student population of the school. The VC is the overall top-most manager of the university; his office and DVCs offices are managing 300 and more staff. The respondents majorly working in the schools of education, business and economics and the school of arts with higher student populations also managed 300 and more staff.

6.4 E-records lifecycle

E-records management is a management function that is vital worldwide and responsible for the efficient and systematic control of e-records processes from creation to disposal (Grant 2014; IRMT 2009, Mutula and Moloi 2007; ISO 2001). The literature reviewed indicated that proper e-records management enhances traceability and verifications of business functions and activities carried out through the proper creation of e-records. Perhaps understanding the business functions is a starting and a continuing point for e-records management. Consequently, the continuum model assists organisations to understand such tasks as determining social and legal requirements for record-keeping, conducting a business process analysis, doing a functional analysis for the classification system, undertaking appraisal and carrying out systems analysis including an overview of the structuring of data about records. E-records are a product of business functions and form among others evidence of the activity from which they were created or received; thus, providing a source of information when facts or knowledge about the structure, operations, process, working methods, personnel, infrastructure among others are needed (Shepherd and Yeo 2003). McKemmish (2001) is of the opinion that use of the records continuum model will lead to the accessibility of meaningful records for as long as they are of value to people, organisations and societies, whether the records are managed for a split second or millennium. This was confirmed from the findings that all the 139 (100%) respondents reported to be involved in various activities of the university in which e-records were created and or received, maintained, stored and preserved by various means including personal computers, information systems, for example financial system, hostel management system, examination system, library system, smartphones, and emails. However, findings from the majority of those interviewed conspicuously indicated that the processes of appraisal and disposal was not practiced in the University. Similarly, the findings from the questionnaires showed lack of knowledge on issues pertaining to appraisal practices and disposal, for example, 99.3% indicated not to be aware of the stage when e-records are appraised, and a significant 94.0% of the respondents reported that there were no guidelines on disposal of e-records. Furthermore, the literature reviewed indicated that functional needs of an organisation, for instance audit, lawsuits, decision making just to mention a few, have to be guided by and not limited to appropriate appraisal scheduling and disposal procedures (ICA 2016; Mukwevho and Lorrette 2013; Kenya public service 2010; National Archives and Records Services of South Africa 2006). Unfortunately, the university lacks the appraisal and disposal procedures which invite a non-conformity 'tag' to its e-records management practices. Although some of the practices of preservation were carried out, the process was understood and used loosely to mean maintenance by majority of the respondents. This is not the case since preservation goes beyond maintenance to providing strategies, approaches, and techniques before and after creation that will sustain e-records in an accessible format so long as a need for those records exists. The literature reviewed also signposted that preservation is planning and taking actions by use of techniques, approaches or strategies and/or with the guidance of a policy in provision of secure storage and integrity of each record manifestation aiming to 'keep' the original e-records intact without changing the technologies used to store or process it. Additionally, maintaining appropriate access control as well as securing offsite storage to offset technology obsolescence of e-records which may involve adopting new technologies that were not in existence when the e-records were originally created (ICA 2016; Handbook of preservation of electronic records 2013; Victorian electronic records strategy 2011; Dressler 2010; Gultenbrunner et al. 2010; Woods and Brown 2010; IRMT 2009; UK National Archives 2006; Boudrez 2005; McKemmish 2005).

Nevertheless, some of the processes such as those of creation and receiving, maintenance and storage are being practiced at Moi University. However, the reviewed literature explains that the process of e-records creation to disposal must be part and parcel of the institutions' process to achieve proper e-records management. The continuum model upholds that e-records management is not about e-records only, but about a regime for record-keeping, which is continuous, dynamic and on-going without any distinct breaks or phases; thus, processes pass seamlessly into another (Shepherd and Yeo 2003; Bantin 2001; McKemmish 2001; Upward 2001).

Furthermore, from the findings e-record-keeping functionalities were not well integrated into the universities' business process systems, as e-records activities were carried out on either single module systems and or in office computers and that there were no laid down guidelines on the same, giving a clear indication of a systemic and procedural problem despite the university being in the processes of finalising an inclusive system that will be able to capture most of the university business processes including but not limited to human resource, academic affairs, and finance. The system was reported to be in the design phase. It will be able to integrate e-record-keeping functions into the business process system referred to as IPPD. Unfortunately not all those interviewed were aware of this undertaking yet they are among the decision makers and essential stakeholders in e-records management matrix. The literature reviewed showed that the project managers or those in authority at the initial phase of a system development will invite all those who will need to make contributions, advice and or critic, suggest and address among others, the issue of record-keeping and its integration in the design of the system (Bantin n.d; ICA 2008). The introduction of a system in the researchers opinion including those of renowned authors as indicated in the literature may not solve or be accepted unless prior sequence of development stages including, but not limited to understanding the organisation business process, understanding user requirements, understanding laws and regulatory requirements, policies and standards, trends in ICTs and infrastructure and financial factors among others (Ernest and Young 2015; Gichoya 2005; Venkatesh, Davis and Davis 2003). However, the literature has lamented on lack of, and inadequate planning when it comes to systems used in e-records management including lack of incorporating the essential processes, controls, and standards needed to regulate the creation, capture, access, and safeguards on a long-term basis of electronic digital records (Kalusopa 2016; Katuu 2015, IRMT 2011; Brown et al. 2009).

In addition, the reviewed literature pointed out that policies, procedures, standards and best practices are essential to ensure that university business needs for evidence, accountability, and information about its activities among others are met. Regrettably, from the findings, all the 139 (100%) respondents reported that there were no specific policies, guidelines or standards on e-records management and security indicating that the process of e-records creation to disposal is being carried out 'haphazardly'. This was as a result of the absence of a well-structured records management programme in the university. Similarly, the findings indicated that e-records management was not well encapsulated in the University's vision, mission or strategic plan.

Availability of ICT policy that guided ICTs operations and the quality manual/procedure that was cascaded from the then ISO 9001 (2008) (which has now been revised to ISO 9001 (2015) was mentioned mainly by the interviewed group. These were said to be part of the documented business process of the university. The findings also showed that the university has principal legal instruments governing the operations of university which included the constitution of Kenya 2010, the University Act 2012, No 42 of 2012, the Moi University Charter 2013, legal notice 2013, legal No 202 of 2013 and the statutes of Moi University 2013, legal notice No 207 of 2013. In this case, one will want to place e-records management among the operations that are guided by the said legislation, but looking at the findings, that is not the case. For instance, ISO 9001 (2015) which the University is compliant to, asserts that the records that have been established by Moi University to provide evidence of conformity to requirements and of the effective operation of the quality management system shall be controlled. Moreover, the university shall establish a documented procedure to define the control needed for the identification, storage, protection, retrieval, retention and disposal of records. In this case, implementation practice may be a significant factor that is hindering the awareness and application of the quality manual.

This concurs with many renowned authors who have lamented on either lack of e-records management legislation and regulatory frameworks or lack or poor implementation policies in most governmental organisations (of which Moi university is part) in the African continent as indicated in the literature reviewed (Katuu 2015; Ngoepe 2014, Mula 2013; Mutula 2013; Nengomasha 2013; Wamukoya 2013; Asongwa 2012; IRMT 2011; Tshotlo and Mjama 2010; Wamukoya and Mutula 2005). Kalusopa (2016), in a study of extent of the integration of Information Communication and Technology (ICT) systems in the management of records in labor organisation in Botswana concurs that there was absence of organisational plans for managing electronic records and legislation, organisational policies, and procedures to guide the management of both paper and electronic records.

Another study by Luyombya (2011) on digital records management in the government of Uganda, concluded that despite the existence of ICT-related policy, a digital records management implementation was lacking. The author further asserts that the records and information technology department, which fell under the ministry of public service, but with statutory responsibility for public records across ministries had not provided advice and leadership in relation to record-keeping best practices and the management of public archives. Luyombya conclusion concurs with the findings of this study that ICT policy was available to guide e-records management practices, but essentially, it only takes care of ICT functionalities, but not those of e-records management. Kyobe, Molai, and Sally (2009) asserted that the failure to capture and preserve e-records in Eastern and Southern African institutions of higher education had been attributed to lack of policies and procedures among other factors.

6.5 Security classification of e-records process handling to facilitate description and access control

E-records are a product and a strategic asset that reflects the business functions of a university. Their security should, therefore, be considered before and after creation to guarantee their safety, thus protecting the universities reputation. The literature reviewed have explained that they are practices designed to prevent e-records at all times from malicious damage, leakage, mishandling, intentional or accidental alteration, deletion, modification of their content, context and structure by having in place proper mechanisms. Each organisation needs to ensure that it protects its e-records assets adequately in all forms during its storage processing and transmission between and within the organisation over both private and public networks. Consequently, they must be satisfied that these assets will be protected properly when they are held or processed by others if a business is conducted more widely (ISO 2002). When there is little or no control over how e-records are secured during and after they are created or received, used, stored, preserved and disposed, inconsistency can lead to difficulties finding and retrieving information (National Archives of Malaysia 2015; Omotosho and Emuonyibofarhe 2014; IRMT 2009; Curtmola et al. 2006; Hu, Ferraiolo and Kuhn 2006; NARA 2005). To guarantee and enhance security, the process should begin before creation and run through all the stages up to disposal. The findings indicated that the university security practices in e-record management was minimal and decentralised. Each department or school has its way of managing security since there are no guidelines and programs to guide e-records security management. Likewise, findings from action officers record managers and records staff showed a significant number (87, 73.7%) of respondents were not satisfied with the security practices, while 31 (26.3%) indicated having more or less satisfaction. The study findings further indicated that the e-records security management component of the organisation functions was represented by the ICT directorate. It was revealed that in the next five years the university was planning to increase funding to the ICT department. The location of e-records within ICT directorate perhaps suggests that the functionalities of records management is thought of as ICT function, which should not be the case. Despite ICT directorate playing a major role in ICT infrastructure, they may not understand well the requirements of e-records security management. The literature reviewed revealed that for successful e-records management, inclusivity of appropriate stakeholders is vital. This is because e-records are by-products of the business process of the university, which should receive adequate attention. The study findings also indicated that e-records security management was not a standalone procedure and was therefore not being audited. However, for the sake of evidence provision during the internal and external audits, the e-records were considered to determine the level of compliance. This is against the literature reviewed which noted that the audit should be used as an initial stage to determine the status of all activities including e-records management (Gullein and Guintero 2007).

Another significant but negative finding was the inadequacy of funding for e-records security management as indicated by 18 (85.7%) of the respondents who were of the opinion that there was no budget for e-records security management; only 3 (14.3%) indicated that there was some money allocated, but meager which they also singled out to be a major concern. The literature reviewed indicated that budgetary allocation and inadequacy of funding towards e-records management and security is a top challenge faced by Kenyan organisations, and indeed, Africa at large (Kenya cybersecurity report 2016; Erima 2013; Mutula 2013; Wamukoya 2013).

The findings from the interviews indicated that analysis of business functions is carried out in Moi University where all 21 (100%) respondents are involved. This response perhaps suggests that functions, process or procedures and activities that lead to creation of e-records of the University are understood and practiced. The literature reviewed indicated that to improve business process, it should be analysed in order to understand the activities, their relationship, and values of their relevant metrics. The literature further indicated that analysis of a business function of an organisation is vital for it links business process to e-records. For instance, personnel involved in the classification of e-records must contend with the fact that e-records should be managed in relation to the business process and the context of other related records. It further indicated that business analysis is a clear way of developing business classification scheme which shows the organisation's activities and transactions in the hierarchical relationship; thus, the need for the development of a classification scheme, which in turn guides e-records security classification

(Wamukoya 2013; Ambira 2010: ICA 2008; State Records New South Wales 2004; ISO 2001; Chinyemba and Ngulube 2005). Similarly, the continuum model observes that business activities are created as part of the business communication process within and without the organisation and advocates for intellectual control of e-records management actions. The e-records management actions include classification or records within a logical system (Upward 2004; Xiaomi 2003; Upward 2001; Miller 1997). This being the case, the university has not fully prioritised e-records security areas and practices including that of developing a classification scheme and written directive on security classification to establish whether the activity and the business area are identified as areas that need more security consideration and legal restrictions. The findings indicated that the University classified its e-records without proper guidelines. The university has also failed to appreciate and initiate or put emphasis on e-records security areas and practices including that of developing a security classification guideline. There neither existed e-records classification scheme nor a documented e-records security classification guide as mentioned earlier. The two documents have different purposes, but they work hand in hand. The functions of e-records classification scheme including that of providing a clear directive on ways and means by which records can be classified including the aim to logically organise e-records created, received and how they are maintained can help in developing a security classification guide (Caravaka 2017). Ngulube and Stilwell (2011) assert that records should be classified wisely according to their subjects to make it easier for users to search for a specific individual subject record/information. The findings indicated that security classification applied is based on the nature of the information and the level at which the e-record was generated. This include 'top secret' (including deliberations of the University Council, students examinations, fiscal matters), 'confidential' (including staff records that is social security numbers, loans and pension records, health records, personnel and pension records, students records), 'Public' (Notices for rallies, workshops, graduations,) and 'internal use' (records used by university staffers and students, internal job advertisements and internal memorandums)'. The literature review provides similar but more security classification techniques depending on the nature of the organisation (Kahanwal and Singh 2013; Mishra 2011; Public Service of Kenya 2010; Yorkland Controls 2007; Collette and Gentile 2006). The guiding principle in e-records security is that the assigned security classification must be appropriate to the content therein; thus, dictating access security control requirements and privileges from e-records inception to disposal (Charles Darwin University 2017).

Security classification thus, dictates the access controls that should or must be applied to e-records to guarantee their security. From the literature reviewed access control is vital, since it helps to protect the assets of the organisation, prevention of illegal entry, enhancement of staff safety, reduction of security cost and facilities management among others. ISO 15489-2 (2001) asserts that the development of appropriate categories of access rights and restrictions is based on the organisation's regulatory framework analysis, business activity analysis and threat assessment where reasonable security and access will depend on both the nature and size of the organisation as well as the content and value of the information requiring security.

Access requirements must be considered to ensure access restrictions and/or access privileges. For instance, there are a variety of devices that can be installed to provide an input for authorised users to open a door or access a specific device, for example, users access cards, keypad input, and biometric information. E-records access controls/restrictions may include among others secure log-in credentials and process, access rights to the approved system, additional levels of security that may be applied to specific records within the system, and level of access (Charles Darwin University 2017; National Archives of Malaysia 2015; ISO/IEC 2014; ISO 2001). The findings indicated that the nature of the business activity determines access status, the role played and individuals' ranking in the university or department. The findings thus, provide a positive attribute that the university practices access control. Unfortunately, the university did not have an access policy to provide directions and guidance on sensitive matters like a user permission register and how the distinction is made on user rights and privileges. The literature reviewed indicated that access policies and or user permission registered are vital and are ways of giving proper directions and or prosecuting those who go against the restrictions.

6.6 Threats to e-records security

E-records security is as much about exploiting the opportunities of our interconnected world as it is about threat management (ISO 2013). Successful organisations and universities understand the value of timely, accurate, good communications and security of e-records. Thus, to identify threats, the assessment process is unavoidable. The initiation of threat assessment requires a proper understanding of the business process and functions of the organisation. The assessment should be able to identify, quantify and prioritise potential e-records security threats against defined criteria for threat acceptance and objectives relevant to the organisation (City University of Hong Kong 2016; ISO/IEC 2013). Findings indicated that threat assessment in the university was achieved through both internal and external audits on the university business processes and that during the process the auditors identify threats to e-records, though it was not adequate in terms of frequency and absence of e-records security policy. The guiding issues on threat included new technologies and their challenges, a document that describes the available information systems, system functions, and boundaries, information about hardware and software, reports from both internal and external audits, self-evaluation, monitoring and through performance contract and quality assurance reports and information about the critical or vital records of the university. The findings from questionnaires generated mixed reactions with most of the respondents (63, 53.4%) indicating that the University never carry out threat assessments. Additionally, 18 (15.3%) reported that assessment is done once per semester, 15 (12.7%) indicated that assessment is done annually and 14 (11.9%) said it is done biannually. Only 8 (6.8%) specified that assessment is done twice per semester.

The evolution and advancement in ICT have brought with it benefits and threats to the technologies, devices used and information generated in equal measure. Though ICT infrastructure does not solve the problem of managing e-records security, availability of ICT is the essential underlying factor for managing e-records (Asogwa 2012; IRMT 2009). The findings indicated that Moi University experiences a number of threats. Foremost, is the lack of a proper e-records management programme to guide the development of policy and procedure in matters of e-records security. Lack of policies and lack of implementation of cascaded regulatory frameworks is also a threat that the university is experiencing. E-records security management at universities should operate within the framework of policies, rules, and procedures that give guidance to practice. The purpose of clear policies and procedures is to provide an environment conducive to proper e-records security. The policies are vital in an environment such as the universities, where the responsibility of e-records security management is distributed among the individual units with little or no centralised control (Bigirimana et al. 2015; Kyobe et al. 2009). The failure to capture and preserve e-records in eastern and southern African institutions of higher education have been attributed to the lack of policies and procedures among other factors (Kemoni 2008; Wamukoya and Mutula 2005). These vital documents allow and help employees to understand their roles concerning the activities stipulated. Their absence indicates that there are no guiding principles and consequently personnel may act with negligence due to ignorance and or lack of awareness, and therefore end up deleting, unauthorised use and illegal sharing or leakage of e-records. This may lead to the university being denied justice in the event of a court case. The findings concur with the literature reviewed where authors, for almost three decades have decried the lack or inadequate policies and procedures in many institutions (Maseh 2015; Lappin 2013; Mutula 2013; Wamukoya 2013; Williams 2013; Asogwa 2012; IRMT 2011; Nengomasha 2009; Kaekopa 2007; Moloi and Mutula 2007; Makhura and Ngulube 2005; Sejane 2005; Wamukoya and Mutula 2005; Wamukoya 1996).

The findings also indicated that personnel were also among the significant threats to e-records security; it was revealed that information leakage and sharing was on the rise including sharing of access privileges and passwords, staff collusion in manipulation and modification of e-records including student marks, stealing of computers and storage devices among others. The literature reviewed indicated that e-records are more vulnerable to undetected alteration, unauthorised disclosure of information, improper or careless handling, accidental erasure or mislabeling of storage devices and physical damage to hardware and software **(**Raaen 2017; Africa Cybersecurity report 2016; Greizter 2014; Ernest and Young 2013; Bey 2012; Dean 2012; Ngoepe et al. 2010; Parker 2002; Parker 1998). Parkerian Hexad Model warns that employees are the primary or most prominent threat to e-records because they understand the technology and the e-records created and received as they are the creators. They sometimes accidentally delete files, enter inaccurate information, save over the wrong files, or edit the wrong files (Parker 2002). The findings further indicated that cyberspace has brought out challenges including cybercriminals (hackers and crackers) who as new technologies emerge, they concurrently or immediately invent and discover new ways to tap in the new technologies with the intention to steal and corrupt e-records for their benefit; thus, hurting organisations' reputation. Also, cyber-attacks including viruses and worms were widely mentioned in the findings as a threat to e-records and the computer system that host them and storage devices. The literature reviewed showed that the globalisation process and the internet revolution has influenced cyberspace across national and international borders making it a complex challenge for any government to address issues of e-records security (Kenya Cybersecurity report 2016; Ministry of ICT, Kenya, 2014; Omotosho and Emuoyibofarhe 2014).

Cyber-attacks have become more organised and more expensive to the economies pausing potential risk and damage to the government administration and the private sector. The attacks include, but are not limited to network-based attacks, social engineering, threats to physical security, attacks targeted to specific applications, information theft and cryptographic attacks (North Atlantic Treaty Organisation (NATO 2010).

According to Kenya Cybersecurity report (2016), between 2012 and 2016 there has been a rapid change in technology and cybersecurity landscapes. According to the report in 2012 cybercriminals were opportunistic compared to 2016 when they are more focused and targeted with their skills. For instance, the literature indicated that the ransomware attack, which affected developed countries and few African countries, targeted organisations' employees (Symantec special report 2016). Similarly, Kaspersky lab report (2016) noted that ransomware attacks increased where the service sector was prominently the most affected business sector at 38% of organisational infections. Manufacturing sector followed with 17% along with real estate and public administration at 10%. Looking at the two reports, Moi University being a service institution is a potential victim and therefore highly targeted.

Kenya Cybersecurity Report (2016) laments that, while there are high levels of investments in technology and automated processes in government services and private sector, there was no matching investment in cyber threat prevention tools. The report further indicates that 96% of the organisations surveyed spend less than USD 5,000 annually or none at all on cybersecurity-related products.

6.7 Measures to protect unauthorised access to e-records

The literature reviewed revealed that organisations have to ensure that e-records are secured at all times from the time of creation or when received, to their disposal. E-records management systems should be able to provide the required functionalities and controls to protect e-records from unauthorised access. Authorised access should only be allowed to workgroups or clearly defined users with a user account and a business need to access e-records (University of Tasmania 2014; Kahanwal and Singh 2013; ISO 2001). The findings of the study indicate that logical controls (use of passwords, PIN, the principle of least privilege, digital signatures, network intrusion detector) and physical controls (Access restrictions to computers and offices to authorised personnel) were being applied to protect e-records from authorised access. Furthermore, the findings indicated that the following practices were encouraged: proper record-keeping process including ensuring the information that is captured is accurate, correct and has no errors; that records are created and managed in folders as per the activity leading to their creation and back up practices encouraged; and observing a continuous assessment on the network. Physical security infrastructure was also reported as having security personnel manning the university premises, the available university buildings and structure were also in the sound architectural state, that is, durable and conducive buildings with burglarproof doors and windows fitted with grills. With this kind of finding, one will want to believe that e-records are secure from intruders, but looking back to the findings in 6.5, personnel are themselves a threat to ICT infrastructure and e-records. That said, the findings indicate that the university appreciates the importance of protecting e-records. The lack of written policies and regulation was noted repeatedly as echoed in section 6.4.

The literature reviewed indicates that as the availability of e-records security becomes increasingly mobile, the possibility of unauthorised access and other malicious threats become larger and larger, which could have adverse effects on organisational operations, assets and personnel, thus causing a disruption of access to or use of e-records and e-records systems. An organisation should, therefore, have in mind the multidisciplinary essence of security with particular emphasis on the active management, participation and the realisation of educational program goals. Record-keeping system whether paper or electronic should include a set of rules that are easily understood and should enable the efficient retrieval of information and block unauthorised access (Tasmania Archive and Heritage Office (TAHO 2015); Omotosho and Emuoyibofarhe 2014; Venafi 2013). The Kenya Computer and Cybercrime Bill (2017), indicates that access by a person to a computer system is unauthorised if that person is not entitled to access of any kind, the person does not have consent from any person who is entitled to access the computer system through any function to the programme or information. The literature further asserts that measures to protect e-records from unauthorised access may occur in many ways, for example, denying entry or exit to having elaborate physical security including locks and keys or security guards, to high tech means (use of biometric readers, keypads, smart cards, anti-passback, CCTVS, password protection, intrusion detection and prevention, security classification labelling and encryption among others (TAHO 2015; Omotosho and Emuoyibofarhe 2014; Venafi 2013; Bandar and Colin 2007; Yorkland control 2007; ISO 2001).

However, having in place only physical security measures such as burglarproof doors, grills on windows, identification cards and tedious sign-out procedures for authorised users will not entirely solve cybersecurity attacks. The findings further indicated that measures available to protect intranet against external and internal cyber-attacks included firewalls, intrusion detection through network surveillance and monitoring, having in place hack-proof network system, antiviruses and use of passwords. However, it was not clear from the findings whether monitoring and reaching out to individual user or departments on the proper use of the internet to minimise cyber-attacks was being done. The literature reviewed indicates that critical controls to protect cyber-attacks may include, but are not limited to, inventory authorised and unauthorised devices, inventory of authorised and unauthorised software, secure configurations for hardware and software on laptops, workstations and servers, secure configurations of network devices such as firewalls, routers and switches, maintenance and analysis of security audit logs, controlled use of administrative privileges and controlled access based on the need to know among others (Glant and Landine 2012).

6.8 E-records confidentiality, integrity, availability, authenticity, possession/control and utility

The findings of the study indicated that ethical values of confidentiality, integrity, availability, authenticity, possession/control and utility are practiced to some extent in the university. However, with the decentralised nature of running of school or department affairs, lack of guiding principles and weak implementation of classification of e-records, the security of the information is the mercy of the department or school. It was revealed that student examination management is typically handled by one ICT personnel and or an administrator in the school with the Dean being the super user when it comes to access. Vetting of the staff was not done in most of the departments and schools to familiarise and sensitise personnel on security ethical values. This suggests that the university lacks clear guidelines on the standard way of sensitising personnel on the security values of confidentiality, integrity, availability, authenticity, possession/control and utility.

The findings showed that unauthorised personnel in the university were potential threats as they could come across confidential e-records during creation or receipt, storage, transfer, usage and maintenance processes. Human resource records and student records were easily leaked and shared unnecessarily. Nevertheless, areas like finance were organised in a way to protect financial records of the university. From the survey questionnaire the findings revealed that 19.7% of the respondents agreed that availability of e-records was achieved, and another 15.9% of the respondents indicated that confidentiality was achieved. Possession/control, authenticity, and utility of e-records averaged at 14% of the respondents, while accessibility and Integrity of e-records came at 11.4% and 10.4% of the respondents respectively. These results suggest that the university performed below par on security ethical values. According to the reviewed literature, any organisation has some form of electronic records that are classified and confidential, which should not be made available or disclosed to unauthorised individuals, entities, or processes/systems. The sentiments are shared by the Parkerian Hexad Model which asserts that confidentiality is the limited observation and disclosure of knowledge and that only authorised access should always be practiced (Parker 2002). The process of protecting confidentiality is limiting who can see 'what', based on level and pre-established role-based privilege. For instance, student records, medical records, social security numbers, personal identification numbers, staff loan records, staff evaluation, salary, birth date, passwords, and logins should be limited to authorised access personnel. This is because breach of confidentiality may be prejudicial to the interests of the organisation and or its users (Northeastern University policy 2018; Bristol clinical commissioning group records management policy 2016; Montclair State University policy; Steichen 2012; Mishra 2011; Parker 2002). Confidentiality according to the literature reviewed is achieved through proper classification, labeling, indexing, and file naming among others (Bigirimana, Jagero and Chizema 2015).

From the findings, integrity of e-records was also not achieved in all instances enlisting personnel as the primary threat to information. For instance, although there were measures to halt unauthorised manipulation of e-records from those with access privileges and those without privileges, cases of modification of student marks were reported from some schools. Improper filing and naming of folders, attacks from viruses which corrupted information among other vices that affect information integrity in the university, were also reported. This implies that integrity is compromised in some sections of the university. Since inaccurate or altered e-records is a hindrance to the University operations, corrupted e-records and breakdowns from attacks by malicious programs is also a setback to the University's existence. In the digital environment, if records are not managed professionally the integrity and value as legal evidence and as an authoritative source of evidence for the university may easily be compromised (Wamukoya, 2013).

Parkerian Hexad Model describes integrity as the completeness, wholeness, and readability of information and that the information remains unchanged from a previous state; thus, information cannot be modified without authorisation (Parker 2002). Correspondingly, the literature reviewed indicates that e-records and the information systems integrity is when records remain a consistent, accurate, complete, unchanged or uncorrupted representation of the initial process (Bey 2012; Antirion 2011; Andress 2011; Carnegie Mellon University 2011; Hintzbergen et al. 2010; Wu 2009; Bhaiji 2008). Thus, the integrity of e-records in the university is predicated on the premise that it has not been subject to unauthorised or undocumented change. The literature and the model discussed have indicated that breach of integrity can be exhibited in different ways including, but not limited to, cyber-attacks, accidental and malicious intent to erase vital e-records, and unauthorised alterations among others. This happens to both small and established organisations. For example, in 2016, the World Anti-Doping Agency (WADA) discovered that it had suffered a breach of integrity. Cybercriminals stole and released the personal information of famous athletes to damage their reputations; however, upon reviewing the archived information, WADA realised that the information that had been leaked was also manipulated (Hart 2017; WADA 2016). This implies that Moi University should be very vigilant in the digital space to protect e-records from the unseen cybercriminal attacks with the help of the fast-developing trends in cybersecurity. As indicated in the literature reviewed, some security procedures that protect information integrity may include, but are not limited to, performing and maintaining backups, firewalls, antivirus soft wares, hashing, and intrusion detection software. Regardless of the type of measure adopted, a full security program must be in place to maintain the integrity of the data, and a system audit trails must be operational. Furthermore, internal audit holds the potential to play a significant role in integrity compliance because of its semi-autonomous standing and function as overseer of an international control mechanism.

The findings further indicated that the University appreciates the value of information in its availability. The results indicated that the university ensures that there is availability and well-maintained ICT infrastructure including the internet to ensure that information resources are available to the users as and when required. This was evidenced in the following departments; finance, accommodation, and examination that are integrated making the access of e-records by concerned stakeholders easy and without a hitch. Parkerian Model defines availability as usability of information for a purpose (Parker 2002). The ‘purpose’ in Moi University includes decision making, budgeting, planning, administrative, academic, research, collaborations among others that the university is undertaking. This implies that users can access and experience desired information in a timely and reliable manner; that the systems are working promptly; and authorised users are not being denied service. The literature indicated that guaranteeing the availability of e-records comprises maintaining both e-records and the systems or systems that contain it and provide it to users (Qadir and Quadri 2016; Frank 2016; Gladden 2015; Bey 2012; Antirion 2011; Wu 2009; Bhaiji 2008; Parker 2002; Parker 1998).

Authenticity is observed to maintain the originality of the e-records since in losing authenticity, information loses value. The University preserves authenticity in many ways according to the findings including: referring to the authors at a given level to allow access, physical control (including security personnel, raised and secure barbed fences and perimeter walls, burglarproof doors, grills on windows, counter barriers, signage restricting access to authorised users) and administrative controls (passwords, firewalls, user identifications). Parkerian Model defines authenticity as validity, conformance and genuineness of information. Thus, the best-practice mechanism behind the records continuum model is the use of an integrated approach for managing records and archives with the goal to guarantee the reliability, authenticity, accuracy, usability, and completeness of records. The literature asserts that an authentic e-record is one that can be proven to be what it purports to be, to have been created or sent by the person purported to have created or sent it and to have been created and sent at the time purported (Raaen 2017; ISO 2001). It also refers to the assurance that a message, transaction, or other exchange of e-records is from the source it claims to be (Clemmer 2010).

The study findings indicated that the university attempts to observe possession or control of their electronic records and ICT infrastructure available. The following measures were listed to be pursued by the university concerning possession or control of e-records; role-based system access privileges in most of the departments and schools, read-only privileges on the website, access passwords, physical access controls and encryption of data across networks was mentioned by ICT personnel. Nonetheless, most respondents indicated not to be aware or were ignorant of the practice to protect their laptops or storage devices despite admitting to previously having lost phone(s), laptop(s) and or storage devices including flash disks, portable hard drives, DVDs, CDS, and memory cards. The literature reviewed and model discussed indicate that possession/control is holding and controlling the physical substrate(s) in which information is embodied where it requires that to have possession of e-record, the user of Moi University devices (computer; storage media, server) must have sole possession. In a case where two different parties, own physical copies of some e-record, the e-record is available to both parties, but neither party ‘possesses' the record. Consequently, neither party acting individually can prevent the creation of additional physical copies of the information or the distribution of such copies to additional parties (Gladden 2015). Parkerian Model concurs that possession is the holding, controlling and having the ability to use information (Parker 2002).

Regarding the utility of e-records and systems, the findings showed that the university advocates for the usefulness of e-records to meet the intent of the functions that led to their creation. For instance, availability of passwords and keys to e-records and the devices that hold them and also allowing access to personnel with privileges was advocated for. However, as stated in the findings, utility is compromised in most cases by individuals with access rights who either may not be available because of unavoidable circumstances or not willing to provide information because of fear of criticism. This may be attributed to the notion that access rights including role-based privileges are taken for granted. The model and literature reviewed imply that utility is the state of being well suited to be employed for a purpose though in most cases it is used interchangeably with availability, which is not the case. E-records may be available and therefore usable, but it does not necessarily have to be in a useful form to be defined as available. An organisation's e-records may meet the five components of the Parkerian Hexad Model of confidentiality, integrity, availability, authenticity, and possession, but not utility. Utility strives to answer the questions, is it useful or is it the right information Moi University needs? This implies that the e-records and the system or devices that hold the information should be in a useful state (having records available in a useful state including having passwords and keys to access the computers). The business process or function of the institution that led to the creation of the information, hence a usable record is one that can be located, retrieved, presented and interpreted (Gladden 2015; Bey 2012; Parker 2010; Parker 2002; ISO 2001).

6.9 Skills and competencies available for e-records security management

Findings indicated that there are adequate personnel involved in e-records management. However, not all of them had professional and academic qualifications from the field of information sciences or specialised in the area of records and archives management. Only those who work in the central registry had requisite qualifications. This implies that professional staff is inadequate in e-records management security at Moi University. The findings indicated that capacity building was inadequate especially with regards to continuous education and training in e-records security management because of inadequate finances/funding and lack of policies and regulatory frameworks in e-records management. Although there was a training policy, implementation was not achieved because of inadequate staff development budget. Similarly, findings from questionnaires, revealed that 80.5% of the respondents reported that there was no training on e-records security management. While some indicated that the school of information science was involved in organising workshops for some schools and departments, which was also confirmed by the dean of the school, lack of goodwill, support and financial constraint has affected the frequency of planning and organising the workshops.

With the advancement of ICTs, information and records management professionals have a responsibility in the e-records security management before and during creation to disposal as well as the systems (single model systems and/or integrated information's systems) which are means of e-records processing from creation to disposal, data mining, content management just to mention a few. The findings revealed that the university is either not acquainted enough with matters regarding e-records security management or there is a lack of goodwill from top management. These sentiments are shared by those discussed in the literature that records management in general and e-records management particularly in the ESARBICA region, is severely under-resourced (both in terms of finance and personnel). The findings of the study specified that records are managed by creators who have no skills or competencies, which has resulted in the lack of professionalism despite recurrent discussions and directions on issues pertaining to skills, competencies, training, and capacity building which many authors have lamented as a matter of concern the world over (Chigariro and Khumalo 2018; Ngoepe 2014; Asogwa 2013; Nengomasha 2013; Asogwa 2012; Mwangi 2012; Mulaudzi et al. 2012; Nyongesa 2012; Xiaomi 2009; Deng Nan 2008; Mnjama and Wamukoya 2007; Johare 2006; Wato 2006; Wamukoya and Mutula 2005; Katuu 2003).

Electronic environment and the challenges that come along with it requires that records and archives management personnel be equipped with new skills and competencies through training and retraining to be able to manage e-records security effectively. This calls for the sharing of responsibility by all professionals to understand the business functions of the University; from the information systems initiation and development to the process of creation to disposal with the aim of capturing the e-record in a static or permanent form that will enable them to provide evidence of Moi university's business functions (Kumar and Bansal 2014; Johare 2006).

With the rapid technological advancement and increased network reach, it is unfortunate that the University is experiencing financial crisis that has led to inadequacy in funding awareness workshops and seminars in matters to do with security and records management. The advancement of technology brings about cyber-attacks, and this calls for frequent if not rapid and continuous awareness in e-records security management. Kenya cybersecurity report (2016) laments that one of the most critical challenges facing Kenyan organisations is lack of awareness among technology users about the level of threats they are exposing themselves to. The Parkerian Model asserts that an organisation should focus on their people (personnel) for they are the creators, users, and maintainers among others of the system. The model emphasises that human resources are very valuable, but also the biggest threat to e-records security. For instance, the Parkerian Model explains that staff can sometimes enter inaccurate information, save over and edit the wrong file, steal or share confidential information, intrude and accidentally delete files. Thus, with the help of the continuum model, the personnel will be able to gain knowledge and skills that extend the concept of the continuum beyond metaphor (Upward 2004).

As indicated in section 6.4, e-records security management has not been captured on the organisation structure of Moi University. This may suggest that this aspect has not being given priority. This may affect budget allocation e-records security management. The International Council of Archives (ICA) and its Eastern and Southern African Regional Branch maintains that staff competencies, skills, and tools needed to manage e-records particularly, have not been adequately developed in many public sector organisations in developing countries. This situation is complicated further by the fact that at the policy level, senior officials and legislators are often unaware of the requirement to the management of electronic records over time so that the evidence base of government will be secure and accessible when needed (Kumar and Bansal 2014).

A study by Ambira (2016) on a framework for management of electronic records in support of e-government in Kenya, asserted that most of the records management officers and other personnel in records management units in Kenyan government were deployed from non-records management units in 2003 following the restructuring by the government with majority coming from supplies departments. The author further indicates that registries were being used as "dumping" grounds for non-performing individuals. Where the author concludes that such actions have contributed to the low skill levels because the individuals in the record management roles were not interested in the practice from the start. This immensely correlates with the findings of this study.

6.10 Summary

This chapter offered an interpretation and discussion of the findings of the study presented in chapter five to provide meaning to the data collected. Areas interpreted and discussed were in relation to the themes gleaned from the research questions of the study. This included understanding the process of e-records creation and the business functions that lead to their generation. Appreciating that record-keeping bears witness to our lives by evidencing, accounting for and memorising our interactions and relationships; thus, placing us in this world (McKemmish 2005).

The chapter further discussed how Moi University e-records is handled and secured taking account the business needs for sharing or restricting information, and the business impacts associated with such needs. The discussion also covered the threat assessment and threats that compromise the security of e-records, especially in the cyberspace. Since there is little or no control over how e-records are secured during and after they are created or received, used, stored, preserved and disposed, inconsistency can lead to difficulties in finding and retrieving information. Therefore, security ethical values including confidentiality, integrity, availability, possession/control and utility were discussed. Also, emphasised was the fact that security ethical values are not sufficient for protecting e-records and their systems unless additional essential security measures including, but not limited to, extensive education and training, awareness and availability of strong policies, procedures and standards are put in place.

CHAPTER SEVEN

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

7.1 Introduction

The previous chapter presented the interpretation and discussion of the study findings. The purpose of the study was to investigate e-records security management at Moi University and come up with strategies for improvement. The study addressed the following research questions:

i. How are e-records created, maintained, stored, preserved and disposed?
ii. How is the security classification of e-records process handled to facilitate description and access control?
iii. What security threats predispose e-records to damage, destruction or misuse at Moi University and how are they ameliorated?
iv. What measures are available to protect unauthorised access to e-records?
v. How is confidentiality, integrity, availability, authenticity, possession or control and utility of e-records achieved?
vi. What skills and competencies are available for e-records security management?

The study was underpinned on the records continuum and the Parkerian Hexad Model. The study was guided by a pragmatic research paradigm using a mixed method approach where both qualitative and quantitative data were collected through interviews and questionnaires respectively. Case study design was adopted. Qualitative data from interviews were subjected to thematic analysis. This involved coding, grouping the data into categories, identifying the themes and relationships among the categories in which the major themes that emerged were compared to determine the pattern of association. Similarly, quantitative data from questionnaires were analysed using Statistical Package for Social Sciences (SPSS version 24) and tabulated by use of descriptive statistics such as means, frequencies, and percentages and presented using bar graphs and tables.

This chapter presents the summary, conclusions, and recommendations of the study. The summary and conclusion are provided to help readers to link with concepts read in the previous chapters with the recommendations of the study.

7.2 Summary from the findings of the study

The summary of findings covers e-records life cycle, security classification of e-records process handling to facilitate description and access control, security threats predisposing e-records to damage, destruction or misuse and how they are ameliorated, measures available to protect unauthorised access to e-records, how confidentiality, integrity, availability, authenticity, possession or control and utility of e-records is achieved, skills and competencies available for e-records security management.

7.2.1 E-records life cycle

E-records are not a stand-alone entity, but a by-product of the universities' business processes or functions. The university core business includes teaching, research, and outreach services. These functions are supported by various specific business processes and activities including academic (admissions, examinations, secretariat services to senate and its committees' as well as deans and its sub-committees', curriculum development, delivery and implementation, timetabling, examinations, processing of certificates, transcripts and provision of library services), research and outreach services (conferences, projects, workshops and seminars, inaugural and public lectures), physical infrastructural development, development and implementation of quality assurance at all levels of the institution, responsible use of university ICT resources to support the university's mission of teaching, administrative duties, University inventory management, procurement services, hiring and training of human resource, legislative awareness and compliance to policy and regulations, management of national and international relations through collaborations, drafting and signing of memorandum of understanding, coordination and facilitation of the activities the University council and its standing and ad hoc committees, planning administration and development of university activities, overall management of the academic administrative affairs of the university, coordinating and overseeing all activities that affect students welfare such as; accommodation, guidance and counselling, as well as on-campus work study programs.

The other functions of the university include, provision of leadership in performance-based management through performance contracting, staff appraisal and rewards, implementation of the university's strategic plan and other operational plans, activities, and services so as to ensure the universities vision, mission and objectives are realised; budgeting and investment matters;

maintenance of the database on the university's human, implementing prudent financial policies and procedures such as accounting procedures, internal audit, and controls, legal functions that include preparation of legal documents, and advising the institution on legal matters among others. The university business processes generate a lot of e-records including student records (such as student register/ population, certificates, transcripts, welfare and disciplinary measures, nominal rolls, class attendance), personnel records (academic qualification, dependents, employment history; staff personal identification and employment numbers, payroll, disciplinary issues, appraisal reports, terms of employment, social security numbers, staff dependents, staff loans, staff contacts and next of kin) internal and external reports and memorandums, minutes and other records of meetings including notices and agenda, collaborations and memoranda of understandings, contracts and agreements, tender records, legal records, medical records, inventory records, policy records, graduation records, and financial records including grants, budgetary records and salary payment. Among the e-records include; performance contract reports, architectural e-records such as maps and building plans among others.

The e-records were created and/received, maintained, stored and preserved by various means including personal computers, information systems for example financial system, hostel management system, examination system, library system, servers, smartphones, and emails. The formats of the e-records generated included PDF, MS office (word, spreadsheets, power points, access) videos and audio files, pictures drawings and markup language used on the university website. However, it was evidenced by research findings that disposal of records was not carried out and, in a few instances, where disposal was carried out, there was no documentation of the same. The university lacks a records management program in general and e-records management program particularly. Furthermore, there was no retention and disposal schedules demonstrating that the University manages its' records as a stand-alone activity through registries with only a few staff trained in records management. The finding revealed that the university desperately lacks a proper guideline to streamline e-records management.

In addition, record-keeping functionalities were not well integrated into the universities business process systems, safe for finance, student information and examination. The University was however, finalising an inclusive system that will be able to capture most of the university business processes including, but not limited to, human resource, academic affairs, and financial affairs.

The university did not have specific policies, guidelines or standards on e-records management and security and consequently, the process of e-records creation to disposal was carried out ‘haphazardly'. Research findings indicated that during audits by ISO represented by KEBS, mostly hard copy records were used as evidence for the activities performed. This agreed with the requirement for implementation of ISO 9001 (2008) standards which advocates for documentation as evidence of activities carried out in the university. The University was however, in the process of implementing ISO 9001 (2015), which advocates for the electronic form of information and services promoting the need for a proper guideline that streamlines e-records management all through the e-records life cycle.

7.2.2 Security classification of e-records process handling to facilitate description and access control

The university security practices in e-record management were minimal and decentralised. Each department and school had its way of managing e-records security since there were no guidelines and programs to give directions on matters of e-records management in general and e-records security management particularly.

E-records security management in the organisation structure was championed by the ICT department. The findings revealed that there was inadequate funding for e-records security management. However, the University planned to increase funding to the ICT department within the next five years and would also intensify advocacy for e-records security. The findings revealed that e-records security management was not a standalone procedure in the university and as a result it was not being audited although, for the sake of evidence provision and formality during the internal and external audits, the e-records were included as part of the audits.

The findings further revealed that even though the analysis of business functions and processes was being carried out in Moi University, the University had failed to appreciate e-records security areas and practices including developing a classification scheme and written directive on security classification. The security classification applied was based on the nature of the information and the level at which the e-record was generated and received. The classification was categorised as ‘top secret’ (including deliberations of the university council and senate, students examinations’, fiscal matters), ‘confidential’ (including staff records that is; social security numbers, loans records, pension records, health records, personnel records, students records among others), ‘Public’ (including notices for rallies, workshops, graduations, internal and external job advertisements) and ‘internal use (records that can only be used by university personnel and students, internal job advertisements)’.

The findings revealed that access control was practiced in the University with the nature of the business activity determining the access status, role-based privileges and the principle of least access, whereby one is only required to access information that is needed rather than everything contained in the database. Regrettably, the university did not have an access policy to provide directions and guidance on sensitive areas such as user permission register and how a distinction was made on user rights and privileges. Vital to e-records management are ways of giving proper guidelines on security classification of e-records process handling to facilitate description and access control.

7.2.3 Threats to e-records security

Threat assessment in the university was carried out albeit unsatisfactory; as a result, Moi University experienced a number of threats. Foremost, was the lack of a proper e-records management programme to guide the development of policy and implementation procedure in matters of e-records security; lack of policies and the lack of implementation of cascaded regulatory frameworks. Due to the lack of policies and guidelines, there was a risk that personnel could act in any way and in the cases where there is a breach of ethical conduct to e-records, employee(s) could feign ignorance and lack of awareness for example in deleting, unauthorised use and illegal sharing/leakage of e-records. Personnel were found as the most significant threat to e-records security. The findings revealed that information leakage and sharing was on the rise including sharing of access privileges and passwords, staff collusion in manipulation and modification of e-records including student marks, stealing of computers and storage devices among others. The findings showed that e-records at Moi University were more vulnerable to undetected alteration, unauthorised disclosure of information, improper or careless handling, accidental erasure or mislabeling of storage devices and physical damage to hardware and software.

The study further identified cyberspace as another security challenge. Cybercriminals (hackers and crackers), when new technologies emerge, they concurrently invent and discover new ways to tap in the new technologies with the intention to steal and corrupt e-records for their benefit; thus, hurting the veracity of e-records University's reputation. Cyber-attacks including an attempted attack on the network, viruses, and worms were widely mentioned in the findings as a threat to both the e-records, and the computer system that host them and storage devices.

7.2.4 Measures to protect unauthorized access to e-records

The findings indicated that logical controls (that is use of passwords, PINs, principle of least privilege, digital signatures, network intrusion detector) and physical controls restricting access to computers and offices to authorised personnel (security personnel, security alarms, well secured doors, windows and perimeter fences, security scanners, CCTV) were being applied to protect e-records from authorised access. Furthermore, the findings indicated that proper record-keeping process were encouraged including ensuring that information captured is accurate, correct and has no errors; records are created and managed in folders as per the activity that leads to their creation and proper back up. Additionally, continuous surveillance on the network was also observed because of the attempts of cyber-attacks. Physical security infrastructure was also reported that included having security personnel manning the university premises, well secured burglarproof doors and windows fitted with grills. The findings also indicated the measures available to protect intranet against external and internal cyber-attacks including firewalls, intrusion detection, and monitoring, having in place hacker proof network systems, antiviruses and use of passwords and regular software updates to protect the intranet against cyber-attacks. Little information was made available from interviews and survey questions on how monitoring and reaching out to individual users or departments on the proper use of the internet to minimise cyber-attacks, was facilitated.

Overall, the findings generally indicated that the university appreciated the importance of protecting records.

7.2.5 E-records confidentiality, integrity, availability, authenticity, possession/ control and utility

The findings indicated that ethical values of confidentiality, integrity, availability, authenticity, possession/control and utility were practiced to some extent in the university. However, with the decentralised nature of running of the university affairs especially in schools and departments and the lack of guiding principles coupled with weak implementation of classification of e-records, the security of the information was left at the mercies of individual staff. Vetting of the staff was not done in most of the departments and schools to familiarise and sensitise personnel on security ethical values. There was therefore no standard way of sensitising personnel on the security values of confidentiality, integrity, availability, authenticity, possession/control and utility. The ethical value of confidentiality of these records was therefore not entirely achieved or guaranteed. The findings indicated that there was leakage of staff information and sometimes student records in the University. However, there was more rigor in terms of protecting financial records compared to human resource records and student records which easily leaked and were shared superfluously.

Moreover, findings indicated that the university appreciates the value of information and its availability. The results indicated that the university ensured there was availability as well as well-maintained ICT infrastructure including the internet to ensure information resources were available when and wherever needed. Concerning information and e-records on areas like finance, accommodation, and examinations, which were integrated could be accessed without a hitch.

Findings showed that authenticity was observed to maintain the originality of the e-records because once authenticity is lost, information loses value. The University preserves authenticity in many ways including referring to the authors at a given level to allow access. Access rights preserved and restricted to authorised staff only, using both physical control (including security personnel, raised and strong perimeter fences, well secured burglarproof doors and windows grills, counter barriers, as well as signage announcing restricted access to authorised persons) and logical controls (passwords, firewalls, user ID).

The findings indicated that the university attempts to observe possession or control of their electronic records and ICT infrastructure available. Role-based privileges were applied in most of the departments and schools. Similarly, read-only privileges on the website were applied and end users can only read and not edit University information, use of passwords, and physical control. Encryption of data across networks was mentioned by ICT personnel as a means to ensure possession and control of electronic information, with an indication that most personnel were not aware or ignorant of the practice to protect their laptops or storage devices despite them admitting to either having lost phone(s), laptop(s) and/ or storage devices including flash disks, portable hard drives, DVDs, CDs, and memory cards. Regarding the utility of e-records, the findings showed that the university advocated for the usefulness of e-records to meet the intent of the functions that led to their creation. For instance, availability of passwords and keys to e-records and the devices that hold them and allowing access to personnel with privileges was emphasised. However, as stated earlier, utility of information was compromised in most cases by individuals with access rights.

7.2.6 Skills and competencies available for e-records security management

Findings indicated that there were adequate personnel involved in e-records management. However, not all of them had professional and academic qualifications from the field of information sciences or specialised in the area of records and archives management. Only those who worked in the central registry had the requisite qualifications. There was minimal training opportunities, workshops, and seminars or even in-house arrangements. This was an indication that capacity building was inadequate especially regarding continuous education and training in e-records security management. This was attributed to the lack of finance and non-existent or weak policies and regulatory frameworks in e-records management. E-records management was not reflected in the organisation structure of Moi University; thus, undermining its prominence in the organisation.

7.3 Conclusions of the study the findings

This section elaborates on the conclusions informed by the findings of the study and interpretation.

7.3.1 E-records lifecycle in their continuum care

The findings showed that all units of the university generate massive records, their management is decentralised where each department or school manages their records. However, the process of creation to the disposal of e-records was not comprehensively adhered to; for example, the processes of preservation, appraisal and disposal were not carried out. The University lacked an e-records management programme in general and more specifically, an e-records security management programme. Although the University had adopted regulatory framework and guidelines manuals developed by the Kenya National Archives including the Public Archive Act and the Public Archive and Documentation Act, a closer examination of these documents exposed their lack of clarity on issues of e-records security management. The findings also indicated the principal legal instruments governing the operations of Moi University that included the constitution of Kenya 2010, the University Act 2012, No. 42 of 2012, the Moi University Charter 2013, legal notice 2013, legal No. 202 of 2013 and the statutes of Moi University 2013, and legal notice No 207 of 2013. However, the university had not cascaded the legal instruments to issues of e-records security management. The findings indicated that there were no policies and procedures for e-records management and e-records security management. In particular, the university lacks e-records classification scheme, documented e-records security classification guideline, appraisal, retention and disposal schedules, preservation policy, security policy, access policy, and a records management standard. The findings further showed that although the university is an ISO certified institution, a standard that advocates for the continual improvement of the quality management system by documenting and controlling records that provide evidence to Moi University, the procedure on e-records management is not adequately understood or practiced. There was also no budget for e-records management provided to schools and departments except for the registries and the ICT directorate who reported to have a budget even though it was considered inadequate. The study concludes that as a result of the absence of a functional record management programme, e-records policy framework, budgetary allocation, and well-structured University Records Management arm headed by a University-wide Records Manager, the e-records management process (from creation to disposal) has not received the professional attention it deserves at Moi University. Consequently, it is difficult to ensure that best practices and standards are followed; thus, undermining the quality of e-records management practices at the University.

7.3.2 Security classification of e-records process handling

The University security practices in e-record management were minimal and decentralised. Each department or school had its way of practicing security, since there were no standard guidelines and programs to guide on matters of e-records management. Additionally, recordkeeping functionalities were not well integrated into the university management system. E-records security functions and practices were represented and championed by the ICT department and the funding for e-records security management practices was inadequate. The study concludes that delegation of e-records security management to ICT directorate, which does not have professionals in e-records management has compromised e-records security management practices. The finding further indicated that despite analysing its business process as indicated in section 6.4, the university has not fully appreciated e-records security management including developing a classification scheme and a written instruction on security classification to provide sensitive records that legally require restrictions and the duration of the restriction. The findings showed that the university had in place access controls that depended on user role privileges and the principle of least privilege. However, the findings pointed out that unauthorised access to classified e-records and systems had been witnessed, caused by personnel with requisite privileges and stolen access credentials belonging to the fellow personnel. These findings implicate personnel as a significant threat to information security.

7.3.3 Threats to e-records security

The university experienced several threats. However, the findings showed that threat assessment was inadequate in terms of frequency. The threats range from the members of staff to cyber-attacks, technological obsolescence, among others like the lack of storage spaces, environmental hazards, lack of enough funding to purchase computers, lost /stolen laptops and damaged computers. The study findings further disclosed that the university had experienced phenomenal growth regarding network coverage and bandwidth which has increased the speed at which e-records are shared within and without the University network. This growth has however, come along with considerable cybersecurity challenges including attacks from virus and worms, theft of information, unnoticed sharing and stealing of information. Other notable threats included: theft of computer, laptops, phones, and storage devices including flash disks, and external hard-drives.

7.3.4 Measures to protect unauthorised access to e-records

The university had in place several measures to protect e-records, networks, and information systems from unauthorised access. The measures practiced by the university included the following: control of physical access to premises through security guards at the entrances, well-secured office blocks and distress security alarms and siren; computer security system plans such as access password protection, end to end encryption of shared data, antivirus and firewall protection; upgrading of systems/soft wares and backup and recovery plans. These measures did, however, not entirely deter multiple attempts of data intrusion on the network, denial of service and unauthorised sharing of user credentials, as well as allowing unauthorised access either to steal, manipulate, and delete information. The study concludes that the university has put considerable effort into the protection of e-records from external aggressions. However, the internal threat to e-records security management posed by personnel remains unattended. Further, cyber-attacks are undoubtedly the major security threats to e-records and should be deterred at all cost to avoid massive loss of information.

7.3.5 E-records confidentiality, integrity, availability, authenticity, possession/ control and utility

According to the research findings, the ethical values of confidentiality, integrity, availability, authenticity, possession/control and utility were not fully achieved, thus, not well practiced. Looking at threats experienced at the university, they involve ethical values to a large extent. The findings indicated that e-records are given administrative rights at various levels with some having higher rights and others having lower rights. In case a user with higher rights is not available, availability of that record is compromised, and this also limits the usefulness of e-records (limiting utility). The findings also indicated that the university lacks a security management policy and standard. The study, therefore, concludes that the ethical values that form important component of e-security management are weakly practiced at the university, and this is fueled by the conspicuous lack in a comprehensive e-security management policy.

7.3.6 Skills and competencies available for e-records security management

The findings also indicated that skills and competencies were inadequate especially regarding continuous education and training and awareness in e-records security management matters. This was attributed to inadequate finance and lack of policy guidance and regulatory frameworks in e-records security management among other things. The findings further revealed that a few staff with required competencies and skills in information and records management were posted at the registry(s). This implies that there was paucity of professional qualification in e-records management security at the university.

7.4 Recommendations

The recommendations proffered here are based on the findings of the study, their, interpretation, and conclusion arising thereof.

7.4.1 Recommendation on e-records lifecycle in their continuum care

The study established that e-records management processes of creation to disposal faced a myriad of challenges, thus undermining e-records management practices at the University.

Recommendation 1: Embracing e-services in the University

Efficient and reliable access to information in paperless form is the current global trend. Adopting electronic based service provision to the university stakeholders will therefore be a good point of departure towards entrenching e-records security practices. This will mean that activities of the university including teaching, research and extension, planning and administration, finance, human resource among others discussed in 7.2.1 will be integrated and services provided at the click of a button. For these activities to run smoothly, a robust integrated e-service management system that guarantees efficiency and reliability of e-records is recommended. This is in recognition of the fact that records are indispensable and a significantly valuable resource, which dictates all the operations of the University. These services should be classified to enhance security as mentioned in recommendation 7. This will also improve issues of access to and use of electronic records as also mentioned in recommendation 8. The University should comprehensively embrace information communication technologies to enhance quality e-services through sound and secure e-records. Furthermore, advocating for provision of e-services will bring with it the merit of sourcing for funds, proper infrastructure to secure the e-records, training among others, which may go well in enhancing e-records management security. However, continued use of paper records at a larger scale, undermines the progression of e-records management practices in general and e-records security management, which should not be the case in this era and time.

Recommendation 2: Develop and implement a functional e-records management programme

Records management cuts across all departments of the university, and they are tools that reflect universities functions, processes, practices, and activities. For instance, being a public institution, funded by the Exchequer, it is mandated by the government of Kenya to provide an elaborate and comprehensive account of events on business functions. Consequently, this can only be achieved by adhering to proper e-records security management practices to avoid audit concerns. Furthermore, the university collaborates with both local and international partners in carrying out various projects; this calls for accountability on the part of University through proper management of electronic records to promote transparency, integrity, fairness, trust, and confidence of the partners funding the projects. Therefore, the university should develop and implement a functional e-records management programme which will help to establish responsibilities and record-keeping requirements for developing and implementing efficient and effective University programmes. This will act as a foundational guide to the university as it transitions fully to e-records management. The stipulation of responsibilities will ensure that personnel of the university comprehend their specific e-records management responsibilities. This will be achieved if the programme incorporates the business process of the organisation and expected e-records to be generated, how they should be managed, used, stored, preserved and disposed considering their security before and after creation. Development of a records management programme may guide the establishment of a fully functional directorate of records and archives management headed by a director with necessary qualifications who will have a university-wide responsibility of championing and implementing an elaborate records management policy framework. Consequently, university management should also consider including management of records in the organisational structure as an indication of responsibility and commitment by the management and the organisation at large towards e-records security management.

Recommendation 3: Implement and cascade regulatory framework and standards

The university should be able to implement and cascade the regulatory frameworks into an operational e-records management program to enhance better practices in the management of e-records. The university should also consider adopting a security management standard ISO/IEC 27001:2014 and also records management standards including ISO 15489:2001, KS 2229:2010-Electronic records management systems-functional requirements; KS ISO/TS 21547:2014 Health informatics-security requirements for archiving electronic health records-guidelines KS2374:2012-Electronic records management systems-implementation guide, KS2391:2013-electronic signatures-metadata requirements, that should be cascaded to fit the business needs of Moi University. For example, the ISO 15489 was designed to guide ISO 9001:2008 which has been revised to 9001:2015 in meeting e-records management requirements within the standard. This will go a long way in streamlining e-records security management practices. However, the university can settle on two of the listed standards to support the cascaded ISO 9001:2015 as a way of enhancing best practices in e-records security management.

Recommendation 4: Develop and implement policies and procedure or schedules

The university should develop e-records management policies that integrate matters of security. The existing regulatory frameworks should guide the university-wide policy formulation. They include e-records classification scheme, documented e-records security classification guideline, appraisal, retention and disposal schedules, preservation policy, security policy, access policy, and/an e-records management policy that encompasses all the procedures and schedules. The policy should apply equally to all personnel of the university, all business process, functions and activities of the university and all records regardless of format created or received in the course of conducting business.

Recommendation 5: Facilitate an adequate budget

To have successful e-records security management, proper budgetary allocation and funding is necessary. The university should be able to facilitate an adequate budget that will sustain the university-wide activities of the directorate of records management. A comprehensive budget will help in the planning and supporting the activities and functions of the directorate including e-records security. The Director Records Management should prepare a detailed budget with justification on why the university should invest in the management of e-records activities. Make a presentation to the top management justifying the rationale behind e-records security management and the importance of embracing proper strategies in ensuring that services provided generate sound e-records. Support and goodwill will ensure success in the implementation of e-records security management programme.

7.4.2 Security classification of e-records process handling

The study revealed that the security practices of analysing the business process of security classifications and access control were inadequately practiced.

Recommendation 6: Initiating collaboration and harmonisation of essential departments

In the formulation of records management policy, Moi University should recognise the multidisciplinary aspect of e-records security management. The process of policy formulation should, therefore, involve the various departments and stakeholders in e-records security management with the emphasis on the active top management participation, records directorate, ICT Directorate, Quality Assurance Directorate, finance division, and all schools' management. Working together is key in the analysis of business processes of the University, development of systems and implementation. This will espouse sustainable and best practices in e-records security management particularly in the development of information systems. The Director Records Management should liaise with mentioned personnel, to allow various contributions and harmonisation of activities from all interested parties to achieve holistic best practices.

Recommendation 7: E-records security classification

The university should develop a records classification procedure that entails viable security classification guideline that outlines the sensitive business process and the e-records that require legal restrictions and the type of restriction being applied, the duration at which the e-records will remain with the classification tag and when declassification will be applied. This should be communicated to all members of staff. The University, therefore, needs to have in place an elaborate process that provides guidelines on the classification of e-records including the legal and disciplinary measures to be carried out against those in breach of laid down procedures.

Recommendation 8: Access and audit controls

The study further recommends the development of security classification guidelines in identifying access controls to e-records, the information systems, and external storage devices. Before applying access control, the records personnel and the systems administrator should understand the business process and functions and the e-records created or received, and then create a user profile based on user role (role-based privileges) — for instance, super user, administrator. Consequently, access control can be set at different levels including drive, folder, and e-record level. Develop access groups in accordance to user level and user role for example members of the university council, members of top management, university senate, deans, schools, or departments. Perhaps, to achieve proper access control, the e-records filing structure should be constructed coherently to ensure that correct access is being applied across the file system. The university should note that clarifying user roles is necessary so that a computer system can limit the actions or operations that a legitimate user can perform. However, this may not stop illegitimate users from accessing e-records and or the systems, since personnel have a habit of sharing user login credentials. Therefore, an access policy should clarify access to records and systems as an exclusively restricted privilege to members of Moi University fraternity with valid access credentials at each level; hence, strict and firm adherence to access policy is expected of all members of staff. Legal and disciplinary measures against those in violation of laid down procedures should be determined, for example, suspension or termination of one right of access. Consequently, access control is a complete security solution for securing e-records and systems when combined with audit control. Auditing is necessary to guarantee that authorised users do not misuse their privileges. Audit control will be able to analyse all the requests and activities of university users in the system and to find out possible attempted or actual violation and imperfections.

7.4.3 Threats to e-records security

The university faced various threats in e-records security management. The following are recommendations to e-records security threats.

Recommendation 9: Threat analysis and assessment

The records management directorate in coordination with ICT directorate, Quality Assurance directorate should conduct a regular threat assessment to evaluate the level and likelihood of threats in e-records security management. For instance, unauthorised access, use, disclosure, disruption, modification or destruction and denial of access to the information systems and the e-records they create/ receive, maintain, store. The e-records threat assessment process should be deliberately inclusive to guarantee due diligence, compliance, and proper documentation of security-related controls and deliberations. The process should also be able to determine mitigation measures of reducing the identified threats. Real-time analysis of threats, including watching the tools that monitor an organisations' local area networks, entry points, databases, and other internal environments should also be a priority. With increasing security threats, Moi University should get abreast of new types of threats that could be detrimental to its business functions and its existence and possible solutions.

Recommendation 10: Integrated and intelligent cybersecurity management service

The university should continuously and consistently appreciate that cyberspace is here to stay. Therefore, the developments in the cyberspace require deliberate spirited efforts and strategies to combat any cybersecurity issues that are certain to come along**;** initiating a comprehensive, integrated and intelligent cybersecurity management service. Consequently, both logical, administrative and physical control needs to be applied. In particular, the university should embrace proactive management of e-records security matters by ensuring it understands its operating environment including ICT infrastructure, personnel, partners, competitors, and clients. This will involve putting measures to detect and identify new and emerging trends including threats in cyberspace, applying radical and continuous internet monitoring and detection methods and process as a mandatory priority of the University, maintaining an accurate inventory of control systems devices and eliminating any exposure of the equipment to external users, firewall server management, issuance and use of digital certificates or similar means of authentication, online verification of users, end to end encryption of shared messages, inventory of authorised and unauthorised devices, inventory of authorised and unauthorised software, secure configurations for hardware and software on the laptops, workstations and servers. The introduction of the cryptographic system, strengthening and advocating digital signatures use, provide necessary infrastructure that can invite the use of biometric devices to control access and to install and frequently updating available relevant security systems.

Recommendation 11: Engaging cyber security consulting firms

The university may also consider outsourcing services from cyber security consulting firms which provides technologies, processes and practices designed to protect computers, networks, programs and e-records from security threats. This will help to identify strength and weaknesses or gaps of the university cyber security state. The consulting firm may also be resourceful in guiding in the maintenance of a robust security program in security compliance with best practices. However, this should be done in a manner that does not predispose the university to risks of surrendering ownership and custody of University e-records to the consulting firms.

7.4.4 Measures to protect unauthorised access to e-records

The university had in place measures to protect information systems, network, and e-records from unauthorised access. However, cyber-attacks and unauthorised disclosure of information by personnel with requisite credentials or allowing unauthorised personnel to manipulate information was a significant hindrance to protecting e-records.

Recommendation 12: Moi University should develop disciplinary procedures for those accessing e-records, the system or the network with no valid authority. One fundamental way of achieving this is by notifying people through notices and signage mounted on the doors directing that unauthorised access is prohibited to avoid and deter the vice. Regular system investigation, interrogation, and audits should also be used to deter unauthorised access as indicated in recommendation 8; auditing is necessary to guarantee that authorised users do not misuse their privileges by trailing their activities on the network or system. The University should also consider the moral persuasion strategy that is, staff are persuaded as opposed to being compelled or always reminded to use the University resources responsibly and legally.

7.4.5 E-records confidentiality, integrity, availability, authenticity, possession/ control and utility

The ethical values of confidentiality, integrity, availability, authenticity, possession/ control and utility were not fully achieved, thus, not well practiced.

Recommendation 13: Security ethical values

The university should consider the application of security ethical values bearing in mind the continuous development in technology**.** Confidentiality, availability, integrity, authenticity, possession/ control and utility are terms used loosely, but their implementation is an uphill task. Each of the six components is unique and complete, with different techniques of securing e-records and their system. The university security policy should be able to have an elaborate exclusive description of each and the techniques that are applied to each to help advance the security of e-records.

7.4.6 Skills and competencies available for e-records security management

The findings also indicated that skills and competencies were inadequate especially regarding continuous education and training and awareness in e-records security management.

Recommendation 14: Education, training, and awareness

Education is the passport to the future, for tomorrow belongs to those who prepare for it today (Malcolm X, n.d). Utter transformation of ICTs calls for continuous promotion of e-records security education, training, and awareness University-wide. The Director Records Management should focus on the capacity building plan for the e-records staff through education, training and awareness needs for university-wide personnel in collaboration with stakeholders as mentioned in recommendation 6. That notwithstanding, the University on a serious note should consider hiring e-records personnel that have attained a required educational qualification in the relevant field of records management; for instance, graduate and professionals from the school of information sciences within and without the university. For those already working as records staff and action officers, the University should organise training and workshops to build and improve their competencies on e-records security management and related issues. Awareness programmes including workshops, campaigns and seminars should be carried out frequently to achieve effectiveness. The university may choose to use the already–trained staff to facilitate attendance by other staff at suitable external training programme, or they may choose to engage trained and experienced professionals from the school of information science.

Further, cyber security training through seminars, workshops, conferences should also be a frequent phenomenon. By looking at the events of cyber space, cybersecurity should be considered an area of interest and perhaps the university should be on the forefront in advocating and facilitating research and technology in the area of cyberspace to enhance awareness in the university, in the country and globally. Acquiring proper skills and knowledge will help personnel remain aware and cautious, while working on any computer gadget to avoid cybercriminal activities. This is vital because personnel are the most vulnerable link to cyber criminals. Therefore, empowering them is an investment to the University's e-records security. This training should be a global target including all staff members from management to support staff, teaching to non-teaching staff.

Recommendation 15: E-records security management practices in the university

Director Records Management should place e-records security management on the university map. This should be done through proper marketing and ensuring visibility of e-records security management in the university. With a well-resourced directorate (having enough funding and adequate qualified personnel), the university should deploy at least two qualified records management staff to each school and department who work under the dean of the school or head of department and report to the Director Records Management to drive and champion the e-records security agenda. This will enhance best practices and help in unifying and harmonising e-records security management practices among others as asserted by the records continuum that in order to efficiently and effectively be able to manage access to any records in any institution, e-record-keeping necessitates a pro-active incessant radical approach. The Director Records Management in liaison with university fraternity should engage in e-records diligence to enhance implementation. This will involve the implementation of e-records security controls (logical control, administrative controls, and physical control) cost control and engaging professionals at all levels all the time.

7.5 Originality and contribution of the study to knowledge

E-records security has become one of the significant challenges in recent times. Consequently, security threats increase solely together with the proliferation of technology globally. Beholding the literature reviewed, many studies in the field of e-records management have been conducted nationally and internationally, which provided useful insights into the current study. However, there is no evidence of the reviewed studies that seem to address the concerns about e-records security management. The literature reviewed had either broad or specific areas of e-records management and included some sections on security in their studies, which were narrow. Consequently, in most cases, security was equated to confidentiality which should not be the case, as confidentiality is one of the parameters in security practices. Further, from the literature, security has always been concentrated at the end of the last stage with minimal priority to e-records management, and that it is a sole information technology function. However, that is also not the case. The study thus, identifies security as an area with multidimensional complexities that invites intelligence of all professionals in different fields from information sciences, computer sciences to engineers to mention but a few, and stakeholders including top management, deans, directors, heads of departments, records managers, actions officers among others. The study recognises the security as a design process that should be considered before and during e-records creation/ receipt to disposal and also during the system development.

To enhance the originality of the study, a theoretical triangulation in the investigation of e-records security management was adopted. The models applied in the study were Records Continuum Model and Parkerian Hexad Model. The originality was also enhanced through use of a robust research methodology that allowed triangulation where data was collected through interviews and questionnaires that ensured high validity and reliability of the results.

The study therefore attempted to look at e-records security management from a holistic perspective by bringing out fundamental principles, which underpin e-records security management; thus, giving a deep insight to the pertinent areas of e-records lifecycle from creation to disposal by identifying e-records needs and application, e-records security practices; including analysis of the business process of the university to enable e-records security classification; to identifying security threats by looking at the effects of cyberspace to cyberattacks. Furthermore, identifying measures that are used to protect authorised access; and security ethical values that of confidentiality, integrity, availability, authenticity, possession, and utility on e-records, information systems, or desktop, laptops and storage devices were also areas of concern. Consequently, e-records security education, training, and awareness as a fundamental need was addressed where its inadequacy was pointed out as disastrous to the universities existence if not addressed. Perhaps education should begin with the simple, but difficult instruction users should adhere to, that of prohibiting them not to share access credentials and also not allowing the unauthorised person from accessing e-records, the systems available or the storage devices. If well practiced, university-wide user involvement in defending the university from security attack will be a norm if not a culture. The revealed significant challenges included lack of e-records management programme, policy framework, inadequate funding, cyberattacks, and identification of personnel as the threat, failure to adhere to security ethical values, as well as inadequate competencies and skills among others. The study recommended development and implementation of a records management programme and policies, adopting relevant standards, understanding cyberspace, adequate budget and funding, capacity building through education and training and strengthening e-records security management practices in the university. It is worth mentioning that areas of security are similar and can easily create repetition in the discussion as observed in this study. However, the study, is significant to the scholarly literature on e-records security.

7.6 Suggestion for further research

This study investigated e-records management at Moi University. The current government of Kenya having gotten into power in 2013 with a promise of digitalising the economy through e-governance (Jubilee Alliance Manifesto, 2013) and Moi University being a public institution funded by the government is therefore a significant component of government's fiscal responsibility whose e-records security practices impacts the goals of the current government in the achievement of a digitalised economy hence e-governance. The researcher, therefore, recommends a further study on e-records security management in support of e-governance in Kenya.

Additionally, the study revealed policy framework cuts across e-records security practices from creation to disposal. In particular, the practices include; security classification, access controls, ethical values, education, and training to mention a few. The study noted that there were no policies to govern the respective components of e-records practices. However, the researcher’s study did not discuss the components or what the necessary policy framework entails. Therefore, the study recommends a study on policy and regulatory frameworks in e-records security management.

REFERENCES

Ambira, M.C. 2016. A framework for management of electronic records in support of E-government in Kenya. Ph.D. Thesis, University of South Africa.

Anderson, T. 2013. Research Paradigms: Ontology, epistemologies, and methods. [online]Available at: https://www.slideshare.net/eLearnCenter/research-methods-uoc-2013 (Accessed 20 December 2017).

Andress, J. 2011. The basics of information security: Understanding the fundamentals of InfoSec in theory and practice. *Elsevier*,1: 5-8.

ARMA 2008. Vital records: identifying, managing and recovering business-critical records. [online]Available at: https://www.arma.org/Bookstore/productdetail.cfm (accessed 12 February 2018).

Asogwa, B. 2013. The Readiness of Universities in Managing Electronic Records. *A study of Three Federal Universities in Nigeria*, 31(40): 792-807.

Asogwa, B. 2012. The challenges of managing e-records in developing countries: implication for records management in Sub-Saharan Africa. *Records management journal*, 22 (3):198-211.

Association of Information and Image Management (AIIM) 2009. Electronic records management –still playing catch up with paper. [online]Available at: https://www.aiim.org (Accessed 18 August2017)

Australian National University 2015. ANU electronic records management system. (ERMS) manual.

Bandar, A. and Colin, F. 2007. Access control requirements for processing electronic health records in Australia. International conferences on business process management BPM 2007: business process management workshop, pp 371-382.

Bantin, P.C. 2009. Strategies for Managing Electronic Records: A New Archival Paradigm? *An Affirmation of our Archival Tradition, [online]*Available at: http://www.indiana.edu/~libarch/ER/macpaper12.pdf (accessed 3 February 2017).

Bantin, P.C. 2002. Implementing an electronic records management program. [online] Available at: https://slideplayer.com/slide/4824946/ (accessed 7 March 2017).

Bantin, P.C. 2001. Strategies for managing electronic records: Anew archival paradigm? An affirmation of our archival traditions*? Archival Issues,* 23 (1998):15-34.

Barifaijo, K.M., Basheka, B. and Oonyu, J., 2010. *How to write a good dissertation / thesis: a guide to graduate studies*. Kampala: New Vision Publishing.

BBC, 2010. Records management policy. [online]Available at: https://www.bbc.co.uk/guidelines/dq/pdf/media/records_management_policy_v1.4.pdf (accessed 9 July 2018).

Becker, C., Rauber A., Heydegger V., Schnasse J., and Thaller M, 2010. Systematic Characterisation of objects in digital preservation: The extensible Characterization language. *Journal of universal computer science*. [online]Available at: http://www.jucs.org/jucs_14_18/systematic_characterisation_of_objects (accessed 25 October 2018).

Bey, P.G. 2012. The Parkerian Hexad: The CIA triad model expanded, (master's thesis), Lewis University.

Bhaiji, Y. 2008. Chapter 1: Overview of network security. [online]Available at: https://www.networkworld.com/article/2274081/chapter-1--overview-of-network-security.html (accessed 25 February, 2017).

Bigirimana, S., Jagero, N. and Chizema, P., 2015. An assessment of the effectiveness of e-records management at the African University, Mutare, Zimbabwe. *British journal of economics, management &trade* 10(1):1-10 ISSN2278-098X.

Blaxter, L., Hughes,C. and Tight, M. 2006. *How to research*. (3rd ed.) Berkshire: Open University Press.

Brauer, K. 2011. Authentication and security aspects in an international multi-user network. Master's thesis. Turku University of applied sciences.

Brown, A., 2008. Care, handling and storage of removable media. [online]Available at: http://www.nationalarchives.gov.uk/documents/information-management/removable-media-care.pdf (accessed 10 April 2017).

Caravaca, M.M. 2017. Elements and relationships within a records classification scheme. *JLIS.it,* 8, 2.

Carnegie Mellon University 2011. Information security essentials. [online]Available at https://www.cmu.edu/iso/aware/presentation/tepperphd.pdf (21 August 2018).

Chachage, B. and Ngulube, P., 2006. Management of business records in Tanzania: an exploratory case study of selected companies. *South African Journal of Information Management, 8*(3):1-18.

Chadwick, A. May, C. 2003. Interaction between States and Citizens in the Age of the Internet: "e-Government" in the United States, Britain, and the European Union. [online]Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-0491.00216

Chapman, C., 2016. Access control and user authentication. [online]Available at https://www.epa.gov/sites/production/files/2016-10/documents/access_control.pdf (accessed 5 March 2018).

Charles Darwin University, 2018. Records management- Security of University records procedures. [online]Available at. http://www.uvm.edu/policies/general_html/recordretention.pdf. (24 August 2018)

Charles Darwin University 2017. Records disposal schedules: higher education teaching and learning of the University of the Charles Darwin University. [online]Available at: https://www.cdu.edu.au/sites/default/files/itms-docs/disposal-schedule-2017.17-charles-darwin-university-higher-education-teaching-and-learning.pdf (24 August 2018).

Cherryholmes, C.C. 1992. Notes on pragmatism and scientific realism. *Educ. Res*. 21: 13-17.

Chigariro, D. and Khumalo, B. N. 2018. Electronic records management research in ESARBICA: a bibliometric study. *Records Management Journal*, 28(2):159-174.

Chinyemba, A. and Ngulube, P. 2005. Managing records at higher education institutions: A case study of University of KwaZulu-Natal, Pietermaritzburg campus. *South African journal of information management*, 7(1)

Codafile 2015. What is EDRM? [online]Available at: http:// www.codafilesoftware.com (accessed 20 March 2017).

Collette, R. and Gentile, M. 2006. Overcoming obstacles to data classification. [online] Available at: https://www.computereconomics.com/article.cfm?id=1117 (Accessed 3, March 2017).

Commonwealth of Australia, 2017. Cybersecurity: The small business best practice guide. [online]Available at: https://www.asbfeo.gov.au/sites/default/files/documents/ASBFEO-cyber-security-research-report.pdf (accessed 3 April 2018).

Cook, K. 1991. Easy to Byte, harder to chew: the second generation of electronic records archivists. *Archiviria,* (Winter 1991-92), pp 202-8.

Cook, T. and Frost E. 1993. The electronic archival programme at the national archives of Canada: Evaluation and critical factors of success. *Archives and museum information,* pp 38-47.

Cox, R. 1994. More than diplomatic: Functional requirements for evidence in recordkeeping, records management journal. 7:1 pp.31-57.

Creswell, J.W., 2014. *A concise introduction to mixed methods research*. USA: SAGE

Creswell, J.W., 2014b. *Educational research: Planning, conducting and evaluating quantitative and qualitative research. Enhanced Pearson e-text version-access card,* 5th ed. Boston: Pearson.

Creswell, J. W., 2009. *Research design: Qualitative, quantitative and mixed methods approaches* 3rd ed. Thousand Oaks, CA: Sage.

Creswell, J.W., 2008. *Educational research: planning, conducting quantitative and qualitative research*, 3rd ed. Pearson Merrill Prentice Hall: New Jersey.

Creswell, J. W. 2003. *Research design: a qualitative, quantitative and mixed method approaches*, 2nd ed. Californian: Sage publications Inc.

Creswell, J. W. (1994). *Research Design: Qualitative and Quantitative Approaches. Thousand Oaks*. CA: Sage.

Curtin, R., Presser, S., and Singer, E., 2005. Telephone survey nonresponse over the past quarter century. *Public opinion quarterly*, 69 (1), pp.87-98.

Cyrille, N.I. 2010. The management of personnel records in the president's office, public service management, government of Tanzania. Mphil thesis.

Dalta, L. 1994. Paradigm Wars: a basis for peaceful coexistence and beyond. In C.S. Reichard., T. and S.F., Rallis (eds). *The qualitative-quantitative debate: New perspectives*. San Fransisco Jossey-Bass. pp. 70-83.

Dardick G.S. 2010. Cyber Forensics Assurance. [online]Available at https://www.researchgate.net/publication/49285204_Cyber_Forensics_Assurance (accessed 21 August 2018).

Dawson, C. 2009. *Introduction to research methods.* Oxford: How to Books Ltd.

Denscombe, M. 2007. *The good research guide for small-scale social research projects* (3rd ed.) Berkshire: Open University Press.

Dressler, V. 2010. Issues on digital preservation and other related topics. [online]Available at: http://blog.case.edu/digitalpreservation/ (accessed 7 august 2018)

Duranti, L. and MacNeil, H. 1996. The protection of the integrity of the electronic records. An overview of the UBC-MAS research Project, *Archivaria* 42:46-57.

Duranti, L. 2010. Concepts, Principles, and Methods for the Management of Electronic Records. *Records management journal*, 20(1):78-95.

Dwoya, N.S. 2014. Implementation of a records management programme at the Kenya Electricity Transmission Company Limited. Master's Thesis: The University of Nairobi.

Edith Cowan University 2002. The Challenge of Electronic Record Keeping. [online]Available at: http://www.scis.ecu/edu.au (accessed 3, March 2017).

Egwunyenga, E.J. 2009. Records keeping in Universities: associated problems and management options in South West Geo-political zone of Nigeria. *International Journal of education and science*, 1(2):109-113.

Eiring, L. 2008. E-records and archives management education, and training: New Challenges and approaches. [online]Available at: http://www.kualalumpur2008.ica.org/en.sessions/electronic-records-a (accessed on 20 January 2017).

Elliott, H.M. 2007. Record integrity and authentication for electronic R&D. [online] Available at https://www.atriumresearch.com/lib45rary/record_authenticationand_integrity.pdf (accessed 3 February 2017)

England national audit office 2017. Ransomware attack's impact on the National Health Service in England. [online] Available at: https://www.google.com/search?client=firefox-d&q=Ransomware+attack%E2%80%99s+impact+on+the+National+Health+Service+in+England+pdf (accessed 1 November 2018).

Erima, J.A. 2013. Aligning records management and risk management with business processes at Moi University, Eldoret, Kenya. A master's thesis.

Eusch, P. 2017. University Records; File Plans: and Retention Creating a Roadmap to Success.[online] Available at: https://www.library.wisc.edu/archives/wp-content/uploads/sites/23/2017/05/2017_UnivRec_FilePln_Ret.pdf (accessed 2 March 2018).

Fink, A. 2010. *Conducting research literature review: From the internet to paper.* Thousand Oaks, CA: Sage Publications.

Flowerday, S. and Von Solms, R. 2007. What constitutes information integrity? *South African Journal of information management,* 9(4):1-14. [online] available at: https://sajim.co.za/index.php/sajim/article/view/201/199 (accessed 5 April 2017).

Franks, P.C. 2016. An introduction to electronic records management. A PowerPoint presentation at the school of library & Information science San Jose state university, San Jose CA.

Garderen, P.V. 2003. Requirements for assessing and maintaining the authenticity of electronic records. [online]Available at: http://www.cdncouncilarchives.ca/atf_requirements_en.pdf (accessed 5 January 2017)

Gichoya, D. 2005. Factors affecting the successful implementation of ICT projects in government. *The electronic journal of e-government*, 3(4): 175-184.

Ginsberg, W. 2013. Retaining and preserving federal records in a digital environment: background and issues for Congress. [online]Available at: https://fas.org/sgp/crs/misc/R43165.pdf (accessed 11 March 2018).

Girona University 2009. The preservation of vital e-records in Universities. [online]Available at: http://www3.udg.edu/arxiu/publiccat/ip3_isym01_catalonia_paper.pdf (accessed 10 January 2018).

Gladden, M. 2015. *A two-dimensional framework of cognitional security for advanced neuroprosthetics: The handbook of information security for advanced neuroprosthetics.* Indianapolis: Synthypnion academic, pp 129-168.

Glavan, L.M. and Vesna, B.V. 2017. Examining the impact of business process orientation on organizational performance: the case of Croatia. *Croatian operational research society*. 8(1):137-165.

Gledhill, M. 2015. The challenges of born-digital records management at the UK National Archives. [online]Available at: http://www.archives.go.jp/english/news/pdf/151106gledhill_en.pdf (accessed 29 September 2018).

Government of South Australia 2010. General disposal schedule 20 for local government records in South Australia [online] Available at: http://www.lga.sa.gov.au/webdata/resources/project/Management - GDS20 - Intro-1.pdf. (accessed 29 September 2017).

Grant, M.J. and Booth, A. 2009. A typology of reviews: an analysis of 14 review types and associated methodologies. *Health information and libraries journal*. 26(2):91-108.

Grants, C. and Osanloo, A. 2014. Understanding, selecting, and integrating a theoretical framework in dissertation research: creating the blueprint for your 'house'. *Administrative issues journal: connecting education, practice, and research*, 4(2).

Greene, J.C., Carecelli, V.J. 2003. Making paradigmatic sense of mixed methods practice. In A. Tashakkori and C. Teddlie (eds.). *Handbook of mixed methods in social and behavioral research*. Thousand Oaks, CA: sage. pp. 91-110.

Greitzer, F.L. 2014. Analysis of unintentional insider threats deriving from social engineering exploits. [online]Available at: https://www.ieeesecurity.org/TC/SPW2014/papers/5103a236.PDF (accessed 25 September 2017).

Gugulethu, S.N., Ngulube, P. and Mangena, S. 2013. E-records readiness at the national archives of Zimbabwe. *Mousaion*, 30(2): 108-116.

Gupta, I.S. 2001. Intranet, Extranet, firewall. Indian Institute of Technology Kharagpur. [online] Available at: http://baburd.com.np/material/II/CH5-InternetExtranetFirewall.pdf (accessed 1 September 2018).

Guttenbrunner, M., Becker, C., and Rauber, A. 2010. Keeping the game alive: Evaluating strategies for the preservation of console video games. *International Journal of digital curation*, 5(1): 147-209. [Online] Available at: https://www.researchgate.net/publication/234114892_Keeping_the_Game_Alive_Evaluating_Strategies_for_the_Preservation_of_Console_Video_Games.

Haris V. 2003. The Challenges of preserving electronic memory overtime. Paper read at E-records Management Conference Sandston, SA; 2003. [online] Available at: http://www.jisc.ac.uk/media/documents/publications/recordsmanbriefin.(accessed 25 February 2017).

Hart, J. 2017. A new era of hacking: 2017 will be the year of the data integrity breach. [online] Available at: https://www.itproportal.com/features/a-new-era-of-hacking-2017-will-be-the-year-of-the-data-integrity-breach/

Hoeven et al., 2007. Emulation for digital preservation in practice: The results. *International Journal of Digital Curation*, 2: 123-132.

Holbrook, L.A., and Krosnick, J.A., and Pfent, A. (2007). The causes and consequences of response rates in surveys by the news media and government contractor survey research firms. [online] Available at: https://pprg.stanford.edu/wp-content/uploads/2007-TSMII-chapter-proof.pdf (accessed September 1, 2018).

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) 2013. Targeted cyber intrusion detection and mitigation strategies. [online]Available at: https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B (accessed October 11, 2018).

International Council of Archives, 2008. Principles and functional requirements for records in electronic office environments. [online]Available at: http://www.adri.gov.au/resources/documents/ICA-M2-ERMS.pdf (accessed 15 May 2018).

International Council of Archives, 2016. Digital preservation in lower resource environments: A core curriculum. [online] Available at https://books.google.co.ke/books/about/Digital_preservation_in_lower_resource_e.html?id=vZj0nQAACAAJ&redir_esc=y (accessed 15 May 2018).

International Council on Archives, 2008. Principles and functional requirements for records in electronic office environments: Module 3. Guidelines and functional requirements for records in business systems. [online] Available at https://www.ica.org. (accessed 9 November, 2018).

International Records Management Trust, 2012. *Public records evidence for ICT/e-government and freedom of information: Kenya court case study*. London, IRMT.

International Records Management Trust, 2009. *Understanding the context of Electronic Records.* London: International Records Management Trust.

International Records Management Trust/International Development Research Centre, 2011. An East African situational analysis. Research report, August 2011. London: IRMT/IDRC.

International Records Management Trust, 1999. *Managing legal records.* London: IRMT.

Ismail, A. 2017. Africa least heat by WannaCry ransomware cyber-attack. [online] Available at: https://www.africanews.com/2017/05/15/africa-least-hit-by-wannacry-ransomware-cyber-attack// (accessed 5 September 2018).

ISO/IEC 27000, 2014. *Information technology-security techniques-information security management systems overview and vocabulary*. Geneva, International Organization for Standardization.

ISO 27002, 2005. *Information Technology-security Techniques-Code of Practice for Information.* Geneva, International Organization for Standardization.

ISO/IEC 15816, 2002. *Information technology- techniques –security information objects for access control.* Geneva, International Organization for Standardization.

ISO 9001:2008. *Quality management systems — Requirements*. Geneva, International Organization for Standardization.

ISO 15489-1, 2001. *Information and documentation –Records Management-Part 1: General*. Geneva, International Organization for Standardization.

ISO 15489-2, 2001. *Information and documentation –Records Management-Part 2: Guidelines*. Geneva, International Organization for Standardization.

Israel, G.D. 1992. Determining sample size. [online]Available at: http://sociology.soc.uoc.gr/socmedia/papageo/metaptyxiakoi/sample_size/samplesize1.pdf (accessed 5 May 2017).

Israel, G.D. 2009. Determining sample size 1(No. PEOD-6). [online]Available at: http://edis.ifas.uf/.edu/pd006 (accessed 5 May 2017).

Jacobs, S. 2011. Securing management and managing security. [online]Available at: http//www.doi.org/10.10021978040947913-ch12(accessed 8 November 2017)

Johare, R., 2006. Education and training in electronic records management: the need for partnership building. In C. Khoo, D. Sinh and A. S. Chaudhey (Eds), *Proceedings of the Asia-Pacific conference on library & information education practice* (A-LIEP 2006), Singapore, pp 541-549. Singapore: School of communication & information, Nanyang Technological University.

Johare, R., Noorman, M., Asmadi, M. and Ghazali, M. 2013. The required information technology skills of Malaysian federal records managers. Paper presented on international conference on information, business and education technology (ICIBIT

2013).

Johare, R. 2006. Education and Training in electronic records management (ERM): the need for partnership building 2006:541-549. [online]Available at: https://repository.arizona.edu/handle/10150/106014 (accessed 01 may 2018).

Jubilee manifesto 2013. Transforming Kenya: Securing Kenya's prosperity [online] Available at: https://www.scribd.com/doc/123569244/The-Harmonised-Jubilee-Coalition-Manifesto (accesses 15 October 2018)

Kabata, V. 2013. Outsourcing records storage to the cloud: challenges and prospects for African records managers and archivists. *Mousaion*, 30 (2): 137-157.

Kabeberi, D. 2015. Cybersecurity perspective from the professional. In Kenya cybersecurity report 2015. [online]Available at: https://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf (Accessed 7 June 2018).

Kahanwal, B. and Singh, P.T. 2013. Towards the framework of information security. [online]Available at: https://arxiv.org/pdf/1312.1460. (accessed 7 May 2018).

Kalusopa, T. 2011. Developing an e-records readiness framework for labour organizations in Botswana. Ph.D. thesis, University of South Africa.

Kalusopa T. 2012. Record management practices in labour organisations in Botswana. South African Journal of Information Management. 14,1

Kalusopa, T. 2016. Extent of the integration of information communication and technology (ICT) systems in the management of records in labour organisations in Botswana. *Journal of the South African society of Archivists*, 49.

Kamatula, G.A. 2010. E-government and electronic records: Challenges and prospects for African records managers and archivists. *ESARBICA journal*, 29:167-164.

Katuu, S. 2016. Managing Digital records in a global environment-an assessment of the landscape of international standards and best practice guidelines. *The electronic library*, 100 (1).

Katuu, S. 2015. Managing records in South Africa's public sector- a review of literature. *Journal of the South African Society of Archivists*, 48: 1-13.

Katuu, S. 2012a. Enterprise content management (ECM) implementation in South Africa. *Records management journal*, 22(1): 37-56.

Katuu, S. 2012b. Enterprise content management (ECM) implementation in South Africa. *Records Management Journal,* 22(1): 1-15.

Keakopa, S. 2007. Policies and procedures for the management of e-records in Botswana, Namibia and South Africa. *ESARBICA Journal,* 26: 70-84.

Kefron digital white paper, 2017. 4 business drivers for electronic records management: managing records shouldn't be viewed as just any expense. [online]Available at https://www.kefron.com/wp-content/uploads/2017/01/Kefron-Digital-Whitepaper_4-Business--Drivers-for-Electronic-Records-Management.pdf (accessed 15 February 2018).

Kemoni, H., 2009. Management of electronic records: Review of empirical studies from the Eastern, South African regional Branch of International Council of Archives, ESARBICA region, *Records Management Journal*, 19(3):190-203.

Kemoni, H. 2008. Theoretical framework and literature review in graduate records management research. *African journal of library, archives and information science,* 18(2):103-117.

Kemoni, H. 2007. Records management practices and service delivery in Kenya. Ph.D. thesis. University of KwaZulu-Natal, Pietermaritzburg.

Kemoni, H. and Ngulube, P. 2008. Relationship between Records Management, public service delivery and the attainment of the United Nations Millennium Development Goals in Kenya. Paper presented at the XIX Bi-Annual East and South Africa Regional Branch of the International Council On archives (ESARBICA) General Conference on Empowering Society with information: Tanzania National Archives (Dare salaam), 18 to 22.

Kemoni, H. and Ngulube, P. 2007. National archives and the effective management of public sector records in Kenya. *Mousaion,* 25(2):120-14

Kemoni, H. and Ngulube, P. 2008. Relationship between records management, public service delivery and the attainment of the United Nations Millennium Development Goals in Kenya. *Information Development,* 24(4):296-306.

Kenya Bureau of Standards 2014. *KS 2229:2010-Electronic records management-systems-functional requirements.* Nairobi: Kenya Bureau of Standards.

Kenya Bureau of standards 2017. List of standards approved by the 115th standards approval committee meeting on 6th July 2017. [online]Available at https://www.kebs.org (accessed 1 September 2018).

Kenya computer and cybercrime bill, 2017. National assembly bills 2017. *Kenya Gazette supplement*, 13th June.

Kenya cybersecurity report, 2016. Achieving cyber security resilience: enhancing visibility and increasing awareness. [online]Available at https://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf(accessed 3 March 2018).

Kenya cybersecurity report, 2015. Achieving Enterprise cyber resilience through situational awareness. [online]Available at https://www.serianu.com/downloads/KenyaCyberSecurityReport2015.pdf (accessed 3 March 2018).

Kenya Ministry of information communications and technology, 2014. National Cybersecurity strategy. [online]Available at: http://2016.connected.go.ke/downloads/NATIONAL%20CYBERSECURITY%20STRATEGY%20HIGH.pdf (accessed 20 May 2017).

Kenya National Bureau of statistics, 2017. Women and Men in Kenya Facts and Figures. [online] Available at: https://www.google.com/search?client=firefox-b-d&ei=2JvQXO7LI4OlwStnZjgDQ&q=Kenya+National+Bureau+of+statistics%2C+2017.+Women+and+Men+in+Kenya+Facts+and+Figures.+&oq=Kenya+National+Bureau+of+statistics%2C+2017.+Women+and+Men+in+Kenya+Facts+and+Figures.+&gs_l=psy-ab.3...152993.152993..154679...0.0..0.234.234.2-1......0....2j1..gws-wiz.......0i71.kU1Tatpzi8c (accessed 2 September 2018).

Komen, B.C. 2012. Management of Personnel Records in Support of Good Governance at the Ministry of Local Government Headquarters, Master's thesis, Moi University.

Kootshabe, T.J., (2011). Preservation of records in selected ministries and departments in Botswana, MARM Dissertation, University of Botswana.

Kothari, C.R. 2011. *Research methodology: methods and techniques*. New Delhi, New Age International (P) Limited Publishers.

Kothari, C.R. 2007. *Research methodology-: methods and techniques*, New Delhi, Wiley Eastern Limited.

Kothari, C.R. 2004. *Research methodology: methods and techniques.* New Delhi, New Age International (P) Limited Publishers.

Kulcu, O. 2009. Evolution of e-records management practices in E-government: A Turkish perspective. [online]Available at: http://www.bby.hacettepe.edu.tr/yayinlar/dosyalar/Evolution_of.pdf (accessed 7 September 2018).

Kumar, M. and Barsal, J. 2014. Capacity-building through digitisation, electronic records management and other means for archives: Indian Scenario. 9th Convention Planner, Assam, Dibrugarh University, 2:25-27.

Kumar, A. and Malhotra, S. 2015. Network security threats and protection model-technical report-CSE-101507. [online]Available at: https://arxiv.org/pdf/1511.00568 (accessed July 2018).

Kumar, M. and Wambugu, S. 2016. A primer on the privacy, security, and confidentiality of electronic records. [online] Available at: https://www.measureevaluation.org/resources/publications/sr-15-128-en (accessed 14 May 2018).

Kumar, R. 2005. *Research methodology: A step by step guide for beginners*. 2nd ed. London, Sage Publication.

Kwatsha, N. 2010. Factors affecting the implementation of an electronic document and records management system. Master thesis. University of Stellenbosch.

Kyobe, M.E., Molai, P. and Salie, T. 2009. Investigating e-records management and compliance with regulatory requirements in a South African University. *South African journal of information management*, 11(1): 1-15.

Laudon, K.C. and Laudon, J.P., 2005. *Essentials of management information systems: managing the digital firm*. 6th ed. New Jersey, Pearson Education.

Laws of Kenya 2016. Access to Information Act. No. of 2016. Published by the National Council for Law reporting with the authority of the Attorney-General. [online]Available at https://www.kenyalaw.org

Lemieux, V.L. 2015. One step forward, two steps backward? Does e-government make governments in developing countries more transparent and accountable? [online]Available at:

https://openknowledge.worldbank.org/bitstream/handle/10986/23647/WDR16-BP-One-Step-Forward-Lemieux.pdf?sequence=1&isAllowed=y. (accessed 20 February 2018).

Lewis-Daniels, L. 2009. Managing e-records without an EDRMS. [online] Available at http://www.systemscope.com/wp-content/uploads/2009/10/Managing-e-records-_-without-an-EDRMS.pdf (accessed 5 April 2018).

Library and Archives of Canada 2018. Governance and record-keeping around the world. [online] Available at: htttp://www.bac-lac.gc.ca/eng/services/government-information-resources/information-management/Pages/governance-recordkeeping-newsletter.aspx (accessed 30 August 2018).

Lipchak, A. and McDonald, J. 2003. E-records readiness and capacity building. Paper presented during the electronic government and electronic records, November 2003. [online] Available at: https://www.irmt.org/download/DOCUME%EI/GLOBAL/discussionpaper.pdf (accessed 20 January 2017).

Luyombya, D. 2010. Framework for effective public digital records management in Uganda. Ph.D. thesis, London, University of College London.

Mackenzie, N. and Knipe, S. 2006. Research dilemmas paradigms, methods, and methodology. *Issues in educational research*, 16 (2): 193-205.

Macleod, J. and Hare, C. 2010. Development of RMJ: A mirror of the development of the profession and discipline of records management. *Records management journal*, 20 (1): 9-40.

Magi, T. 2008. A study of US library director’s confidence and practice part on confidentiality. *Library management,* 29(8/9):746-756.

Majinge, M.M. 2014. Investigated Library services provision for people with visual impairment and wheelchairs in academic libraries in Tanzania, Ph.D. Thesis, South Africa, University of KwaZulu-Natal.

Makhura, M. 2005. E-records management in a service organization. Master's Thesis. South Africa: University of Johannesburg.

Makhura, M.M. 2005. The contribution of records management towards an organization's competitive performance. Ph.D. Thesis. South Africa: University of Johannesburg.

Malcolm, X. 1990. Malcolm X speaks: selected speeches and statements. Groove press

Mampe, G.T. and Kalusopa, T. 2012. Records management and service deliver: the case of department of corporate services in the ministry of health Botswana. *Journal of South African society of Archivists,* 45:1-23.

Marshall, C. and Rossman, G.B. 2010. *Designing qualitative research.* 5th edition. London, Sage.

Martin, A. and Khazanchi, D. 2006. Information availability and security policy. Proceedings of the twelfth Americas conference on information systems, Acapulco, Mexico August 04th-06th , 1257-1268.

Marutha, N.S. and Ngulube, P. (2012) in a study of e-records and medical record-keeping practice in the public health sector of the Limpopo Province in South Africa. *Journal of South African society of Archivists,* 45: 39-67.

Marutha, N.S. 2016. A framework to embed medical records management into the healthcare service delivery in Limpopo province of South Africa. Ph.D. thesis. University of Pretoria.

Marzigliano, L., n.d. Advice: Security vs. Utility. [online] Available at: http://www.zigthis.com/145 (accessed 1 March 2017).

Maseh, E. 2015. Records management readiness for open government in the Kenyan Judiciary, Ph.D. Thesis, South Africa, University of KwaZulu-Natal.

Massachusetts public records law n.d. Electronic records management guidelines. [online]Available at: https://www.sec.state.ma.us/arc/arcpdf/Electronic_Records_Guidelines.pdf (accessed 2 July 2018).

Mathipa, E.R. 2015. Reviewing of pertinent literature in research. In E. Mathipa and M. Gumbo. *Addressing research challenges: making headway for developing researchers,* (pp. 22-42). Noordwyk: Mosala-MASEDI Publishers & Booksellers.

McKemmish, S. 2001. Placing records continuum theory and practice. *Archival sciences*, 1: 333-359.

McKemmish, S. 1997. Today, Today and Tomorrow: A Continuum of Responsibility. Proceedings of the Records Management Association of Australia 14th National Convention, 15-17 September 1997. Perth: RMAA.

Mckemmish, S. 1997. Placing records continuum theory and practice. *Journal of archival sciences,* 1 (4): 333-359.

McKim, C.A. 2015. The value of mixed methods research: a mixed method study. *Journal of mixed method research,* 11(2).

Mcleod, J. 2008. Records management research-perspectives and directions. *Journal of society of archivists,* 29(1): 29-40.

Mcleod, J., Childs, S. and Heaford, S. 2007. Records management capacity and compliance toolkits: a critical assessment. Records Management Journal, 17(3). pp. 216-232. ISSN 0956-5698

Microsoft 2009. Virtual private networking: an overview. [online]Available at: https://www.sciencedirect.com/topics/computer-science/virtual-private-network (accessed 11 October 2018).

Microsoft 2017. Ransomware cyber-attack a wake-up call, Microsoft warns. [online]Available at: https://www.treyfin.co.za/wp-content/uploads/2017/.../wannacry-ransomware-15-05-17.pdf (accessed October 11, 2018).

Microsoft 2017. Strong passwords. [online]Available at: htts://docs.microsoft.com/en-us/sql/relational-databases/security/strong-passwords?view=sql-server-2017 (accessed October 11, 2018).

Microsoft 2017. Technology decisions for enabling BYOD with Microsoft enterprise Mobility and security. [online]Available at: https://docs.microsoft.com/en-us/intune/byod-technology-decisions (October 11, 2018).

Migiro, S.O. and Magangi, B.A. 2011. Mixed methods: A review of literature and the future of the new research paradigm. *African Journal of Business Management,* 5(10): 3757-3764.

Miller, L. 2003. *The Right to information-the right to records: the relationship between Mixed approaches,* 3rd ed. Thousand Oaks, CA, Sage Publications.

Ministry of Education 2017. Directorate of University education. [online]Available at: http://education.go.ke/index.php/site-login/education-news/87-plans-on-course-to-fast-track-a-garment-making-cluster-project-in-kisumu-county (accessed 11 December, 2018)

Minnesota State archives 2012. Electronic records management guidelines version 5. [online]Available at:

http://www.mnhs.org/preserve/records/electronicrecords/docs_pdfs/ElectronicRecordsManagementGuidelines032012_V5_Full_001.pdf (accessed 19 April 2017).

Mishra, A.K. 2011. *Information security and Cyber Laws.* New Delhi, S.K. & Sons Publishers.

Mitchel, A. 2012. Writing a good PhD proposal. [online]Available at: https://100thousandwords.wordpress.com/2011/03/04/writing-a-good-phd-proposal-%E2%80%93-some-guidelines-by-dr-audra-mitchell-university-of-york/ (accessed 18 February 2017).

Mnjama, N. and Wamukoya, J. 2007. E-government and records management: an assessment tool for E-records Readiness in Government. *Electronic library*, 25 (3): 274-284.

Moi University 2014. ISO 9001: 2008 Surveillance Audit Report on Moi University- Main Campus conducted by KEBS.

Moi University 2011. Information Communication Technology policy. Moi University Press.

Moi University 2013. ISO 9001: 2008 Surveillance Audit Report on Moi University- Main Campus conducted by KEBS.

Moi University 2013. Quality Manual Procedures. Moi University Press.

Moi University 2013. Strategic Plan 2009/10-2014/15 (Revised). Moi University Press.

Moloi, J. and Mutula, S. 2007. E-records management in an e-government setting in Botswana. *Records management journal*, 24 (4): 290-306.

Montclair State University 2015. Responsible use of university computing resources policy document. *Data classification and Handling (Safeguarding sensitive and confidential information).* [online] Available at: https://www.montclair.edu/information-technology/wp-content/uploads/sites/168/2018/04/DataClassificationandHandlingPolicy.pdf (accessed 3 April 2018).

MoReq 2001. Model requirements specification for the management of electronic records. [online]Available at: http://ec.europa.eu/idabc/servlets/Doc1faf.pdf?id=16847(accessed 11 April 2017).

Moseti, M.I. 2015. Strategies for managing scholarly content at Universities in Kenya. Ph.D. Thesis, South Africa, University of KwaZulu-Natal.

Mudarri, T. and Al-Rabeei, S.A. 2015. Security Fundamentals: access control models. *International Journal of interdisciplinary in theory and practice*, 2344-2409.

Mukwevho, J. and Lorette, J. 2013. The importance of the quality of electronic records management in enhancing accountability in the South Africa public service: A case study of a national department. *Mousion*, 30(2):33-47.

Mullon, P. 2004. Records Management Crucial to Sustain Services.IMIESA.

Musembe, C.N. 2015. Enhancing Records Management for Quality Services in Moi University, Eldoret, Kenya. A master's thesis.

Mutero, J. (2011) "Mobilising Pension Assets for Housing Finance Needs in Africa -- Experience and Prospects in East Africa" in Housing Finance International, Summer 2011: 15-22

Mutiti, N. 2002. Computerization of Archives and Records in the ESARBICA Region. *ESARBICA Journal*, 21:114-119.

Mutiti, N. 2001. The challenges of managing electronic records in the ESARBICA region. *ESARBICA Journal*, 21:56-58.

Mutula, S. and Mostert, J. 2010. Challenges and opportunities of e-government in South Africa. [online]Available at: https://www.researchgate.net/publication/220677195_Challenges_and_opportunities_of_e-government_in_South_Africa/download (accessed 10 August 2018).

Mutula, S.M. 2013. E-government implementation strategies and best practices: Implications for Sub-Saharan Africa. *Mousion*, 30 (2): 5-23.

Myler, E. and Broadbent, G. 2006. ISO/IEC 177799: Standard for information security: Best practice. *Information management journal*, 40 (6): 43-52.

Namande, B.W. 2011. Digitization of archival records: the KNADS experience. Proceedings of the 2nd international conference on African Digital Libraries and Archives (ICADLA_2) South Africa, November.

Nan, D. 2008. Project team of study of electronic records management mechanisms, report on enhancing scientific management of electronic records for China, the China Association for Science and Technology Document 35 July 22, Unpublished.

Nasieku, P. 2010. Management of electronic records at Moi University, Eldoret. Mphil thesis. Moi University.

National Archives and Records Administration 2018. Criteria for successfully managing permanent electronic records. [online]Available at https://www.archives.gov/files/records-mgmt/2019-perm-electronic-records-success-criteria.pdf (accessed 7 February 2018).

National Archives and Records Administration 2011. Electronic records management guidelines. [online]Available at: https//www.sec.state.ma.us/arc/arcpdf/electronic_records_guidelines.pdf (accessed 7 February, 2018).

National Archives and Records Administration 2011. Records management self-assessment report: an assessment of records management programs in the federal government. [online]Available at https://www.archives.gov/files/records-mgnt/resources/self-assessment.pdf (accessed 7 February 2018).

National Archives and Records Administration 2006. Information security oversight office report to the president. [online]Available at https://www.archives.gov/files/isoo/reports/2006-annual-report.pdf (accessed 7 February 2018).

National Archives and Records of South Africa 2006. *Managing E-records in Government Bodies: Policy, Principles and requirements*. 2nd ed. Pretoria, National Archives of South Africa.

National Archives of Australia 2014. Managing your agency records. [online]Available at http://www.naa.gov.au/records-management/agency/index.aspx (accessed 5 April 2017).

National Archives of Australia 2004. Digital Recordkeeping Guidelines digital recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records. *National Archives of Australia, Sydney*. [online]Available at: https://mayaarbinaginting.weebly.com/uploads/1/0/6/1/10612501/digital_recordkeeping.pdf (accessed 5 April 2017).

National Archives of Malaysia, 2011. Electronic records management systems-system specifications for public offices. [online] Available at: http://www.jpm.gov.my/sites/default/files/u290/ELECTRONIC%20RECORDS%20MANAGEMENT%20SYSTEMS%20-%20SYSTEMS%20SPECIFICATION.pdf (accessed 17 July 2018).

Nengomasha, C.T. 2013. The present and future of records and archives management in Sub-Saharan Africa. *Journal of the South African society of archivists*. 4: 2-11.

Nengomasha, C.T. 2009.Managing public sector records in Namibia: a proposal model. *Information development journal*, 25 (2): 112-126.

New South Wales government, 2012. FQAs about ERMS. [online]Available at http://www.records.nsw.gov.au. (accessed 20 March 2017).

Newman, M.E.J., 2006. Modularity and community structure in networks. Proceedings of the national academy of Sciences of the United States of America, 103: 8577-8582.

Newton, C., 1989. Future of records management. In E., Peter, Ed. *how to manage your records: a guide to effective practice.* Cambridge: ICSA publishing.

Ngoepe, M. 2015. Deployment of open source electronic content management software in national government departments in South Africa. Journal of Science and Technology Policy Management. [online] Available at: https://www.emerald.com/insight/content/doi/10.1108/JSTPM-05-2014-0021/full/html

Ngoepe, M., Mokoena, L. and Ngulube, P., 2013. Security, Privacy and ethics in Electronic records management in the South African public sector. *ESARBICA Journal,* 29: 36-66.

Ngoepe, M.S., 2014. Records management models in the public sector in South Africa: is there a flicker of light at the end of the dark tunnel? Paper presented at the South Africa Society of Archivist (SASA) archival conference on archives and records management continuity in sub-Saharan Africa, Durban, July.

Ngulube, P. 2007. The Nature and Accessibility of E-Government in Sub-Sahara Africa. *International Review of Information Ethics*, 7:1-13.

Ngulube, P. 2010. A list opportunity to foster e-democracy and service delivery: E-government in sub-Saharan Africa. *ESARBICA journal,* 29:184-200.

Ngulube, P. 2015. Trends in Research Methodological Procedures used in Knowledge Management Studies. *Afri. J. Lib. Arch & Inf.Sc*., 25 (2): 125-143.

Ngulube, P. and Ngulube, B. 2017. Application and contribution of hermeneutic and eidetic phenomenology to indigenous knowledge research, In P. Ngulube, Ed. *Handbook of research on theoretical perspectives on indigenous knowledge systems in developing countries*. Hershey PA: IGI Global (in Press).

Nkala, G.S., Ngulube, P. and Sikhulumani, B.M. 2012. E-records readiness at the national archives of Zimbabwe. *Mousion,* 30(2):108—116.

Northeastern University, 2018. Policy on confidentiality of university records and information.

[online]Available at: https://www.northeastern.edu/policies/pdfs/Policy_on_Confidentiality_of_University_Records_and_Information.pdf (accessed 23 September 2017).

North Dakota information technology department 2013. Electronic Records Management. [online]Available at: https://www.nd.gov/itd/services/records-management-program/electronic-records-management. (accessed 23 September 2017)

Nunnally, J.C. 1978. *Psychometric theory*, 2nd ed. New York: McGraw-Hill. p 245.

Ohio State University 2011. Electronic records management challenges. [online]Available at https://library.osu.edu/osu-records-management/challenges (accessed 23 September 2017).

Omotosho A. and Emuoyibofarhe, J. 2014. A criticism of the current security, privacy and accountability issues in electronic health records. *International journal of applied information systems*. Foundation of computer science FCS, New York, USA,7(8).

Onwuegbuzie, A.J. and Burke J.R. 2006. The validity issue in mixed research. *Research in schools*, 13(1): 48-63.

Parker, D.B. 2002. Motivating the workforce to support security objectives: Long-term view. In *Fighting computer crime: a new framework for protecting information*. John Wiley & Sons.

Parker, D.B. 1998. *Fighting computer crime: A new framework for protecting information*. New York, Wiley computer publishing, John Wiley & Sons, Inc.

Parker, D.B. 2010. Our excessively simplistic information security model and how to fix it. *ISSA journal*, 12-21.

Parker, D.B. 2007. Risks of risk base security. Communication of ACM.50,(3): 120

Patton, M.Q. 2002. *Qualitative research and evaluation methods.* 3rd ed. Thousand oaks, CA, Sage Publication.

Payne, G. and Payne J. 2004. *Key concepts in social research*. London, Sage Publication.

Polit, D.F. and Beck, C.T. 2004. *Nursing research: Principles and Methods.* 7th ed. Philadelphia, Lippincott.

Public Service of Kenya, 2010. Records Management Procedures. Manual for the Public Service.

Raaen, N. 2017. *Electronic records management guide for the Judiciary*. National Association for court management.

Rajalampi, M. 2011. The role of the intranet in enhancing communication and knowledge sharing in a multinational company: Create, store, retrieve, transfer, use and share information. Master Thesis. Aalto University.

Rehbein, M. 2013. Electronic records management strategies. [online]Available at: http://www.masbo.com/files/CONFERENCES/6_13%20Electronic_Records_Management_Strategies.pdf (accessed 2 July 2018).

Reid, C.R. and Gilbert, H.A., 2010. Using the Parkerian Hexad to introduce security in an information literacy class. Published in proceedings inforsec CD 10 2010. Information security curriculum development conference, pp 45-47.

Relyea, H.C. 2002. E-government: introduction and overview. *Government information quarterly,* 19:9-35.

Ridley, D. 2008. *The literature review: a step-by-step guide for students.* Thousand Oaks, CA, Sage Publication.

Robek, M.F., Brown, G.F. and Stephens, D.O. 1996. *Information and records management document-based information systems.* New York, Glenncoe/McGraw-Hill.

Rogers, C. 2015. Virtual authenticity: Authenticity of digital records from theory to practice. Ph.D. thesis. The University of British Colombia.

Rogers, C. 2016. A literature review of authenticity of records in digital systems from 'machine-readable 'to records in the cloud. *Acervo, Rio De Janeiro,* 29 (2): 16-44.

Rossman, G.B. and Wilson B.L. 1985. Numbers and words: combining qualitative and quantitative methods in a single large-scale evaluation study. *Eval. Rev*, 9: 627.

Saunders, M., Lewis, P. and Thornhill, A. 2012. *Research methods for business students*. London, Pearson education.

Search Engine Optimization (SEO)., 2012. Guidelines on creation and collection of records. [online]Available at: https://www.grs.gov.hk/pdf/gccr_(Eng_only).pdf

Serem, D. K., Boit, J.M. and Wanyama, M.N. 2013. *Understanding research: a simplified form.* Eldoret, Utafiti foundation.

Shaw, A. and Shaw, D.T. 2006. E-records management criteria and information security. Proceeding of 7th Australian information warfare and security conference, Edith Cowan University Perth Western Australia, 4th -5th December 2006.

Shepherd, E. and Yeo, G. 2003. *Managing Records: A handbook of principles and Practice.* London, Facet Publishing.

Shepherd, E. 2006. Why are records in the public sector organizational assets? *Records management journal*, 16(1): 6-12.

Shunda, N. 2007. What is a literature review? (and how do I right one). [online]Available at: https://www.google.com/search?client=firefox-b-d&q=web2.uconn.edu%2Fciom%2FShunda%2FLitRev.pdf (accessed 3 September 2018).

Sichalwe, E.N. 2010. The significance of records management to fostering accountability in the public service reform programme of Tanzania. Ph.D. thesis. South Africa: University of KwaZulu-Natal.

Sichalwe, E.N., Ngulube, P. and Stilwell, C. 2011. Managing records as a strategic resource in the government ministries of Tanzania. *SAGE journals,* 27 (4): 264-279.

Sichwalwe, N.E. 2010. The significance of records Management to fostering accountability in the public service reform programme of Tanzania, Ph.D. Thesis, South Africa, University of KwaZulu-Natal.

Soyka, A.H. 2015. Records as force multiplier: Understanding the records continuum as a framework for examining the role of records in a community. Ph.D. Thesis. University of Pittsburgh.

Spiteri, L. 2012. Records continuum model. [online]Available at: https://www.slideshare.net/CentreforAdvancedMan/records-continuum-model-64433567 (accessed 25 October 2017).

State of California records management program 2002. Electronic records management handbook. [online]Available at: https://www.google.com/search?client=firefox-b-d&q=https%3A%2F%2Fwww.documents.+dgs.ca.gov%2Fosp%2Frecs%2Fermhbkall.pdf (accessed 11 October 2018).

State of Florida, 2010. Electronic records and records management practices. [online]Available at: https://dos.myflorida.com/media/31109/electronicrecordsmanagementpractices. Pdf (accesses 16 January 2018).

Staut, K. 2017. Methods, methodology and madness: Digital records management in the Australia government. *Records management journal*, 27(2): 223-232.

Steichen, P. 2012. Principles and fundamentals of security methodologies of information systems-introduction. [online]Available at: https://www.scribd.com/document/48899546/ISO-IEC-27002 -2005 (accessed 27 January 2017).

Svard, P. 2011. The interface between enterprise content management and records management in changing organizations. Ph.D. dissertation. Mid Sweden University.

Symantec internet security threat report (ISTR) 2016. Ransomware and business. [online]Available at: https://www.symantic.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and _business.pdf.

Tale, S. and Alefaio, O. 2005. Records management in developing countries: challenges and threats-towards a realistic plan. *National archives of Fiji*. [online]Available at: https://acarm.org/documents/issue37/37.6%20Records%20Management%20in%20D (accessed 10 February 2017).

Tasmania Archive and Heritage Office, 2015. Information management advice 34 implementing information security classification in EDRMS. [online]Available at: https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Advice%2034%20Implementing%20Information%20Security%20Classification%20in%20EDRMS.pdf. (accessed 3 September 2017).

Tavakol, M. 2011. Making Sense of Cronbach's Alpha. *International Journal of Medical Education*. 2:53-55.

Technology Excellence in Government, 2000. E-government: integrating electronic records management into enterprise information management. [online]Available at: http://www.reuter.net/teg/erm.htm (accessed 3 March 2017).

Teddlie, C. and Tashakkori, A. 2009. *Foundations of mixed methods research: integrating quantitative and qualitative approaches in the social and behavioural sciences*. Thousand Oaks, CA, Sage Publications.

Terell, S.R. 2012. Mixed –methods research methodologies. *Research in the schools,* 13(1): 48-63.

The national archives of London 2011. Guide 8: disposal of records. [online]Available at: www. Justice.gov.uk/guidance/docs/foi-section-46-code-of-practice.pdf (accessed 5 June 2018).

Thurston, A. 2012. Trustworthy records and open data. *The journal of community informatics*, 2. [online] Available at: https://www.google.com/search?client=firefox-b-d&q=Thurston%2C+A.+2012.+Trustworthy+records+and+open+data.+The+journal+of+community+informatics (accessed 20 May 2018).

Tshotlo, K. and Mnjama, N. 2010. Records management audit: The case of Gaborone City. *ESARBICA Journal*, 29: 5-35.

United Nations Programme on HIV/AIDS (UNAIDS) guidance, 2016. The privacy, confidentiality and security assessment tool: protecting personal health information. [online]Available at: http://www.unaids.org/en/resources/documents/2019/confidentiality_security_assessment_tool (accessed 20 January 2018).

United state department of transportation 2014. [online] Available at https://www./transportation.gov/ (accessed August 12, 2018).

United States Computer Emergency Readiness Team (US-CERT) security tips (ST04-002) 2018. Choosing and protecting passwords. [online] Available at: https://www.us-cert.gov/ncas/tips/ST04-002 (accessed October 11 2018).

United States Computer Emergency Readiness Team (US-CERT) security tips (ST05-012) 2018. Supplementing passwords. [online] Available at: https://www.us-cert.gov/ncas/tips/ST05-012 (accessed October 11 2018).

United States Computer Emergency Readiness Team (US-CERT) security tips (ST05-017) 2018. Cybersecurity for electronic devices. [online]Available at: https://www.us-cert.gov/ncas/tips/ST05-017 (accessed October 11 2018).

United States National Archives 2004. Electronic Records management guidance on methodology for determining agency-unique requirements. [online]Available at: https://www.archives.gov/records-mgmt/policy/requirements-guidance.html (accessed 16 November 2017).

University of Canterbury 2015. Records management policy. [online]Available at: https://www.canterbury.ac.nz/media/uc-policy-library/general/Records-Management-Policy.pdf (accessed 3 April 2018).

University of Edinburgh 2011. Electronic preservation strategy. [online]Available at: www.lib.ed.ac.uk/resources/collections/specdivision/criteria.pdf (accessed 23 July 2018).

University of Minnesota Press 2003. The moving image. 3(2):100-107.

University of Nottingham 2015. Guide document: New staff induction-Records management framework. [online]Available at: https://www.nottingham.ac.k/governance/records.management/document/guidance. (accessed 25 February 2018).

University of Tasmania 2014. Records security guidelines. [online]Available at: https://www.utas.edu.au/__data/assets/pdf_file/0020/533612/Records-Security-Guidelines-May-2014-minor-amendments-December-2016.pdf (accessed 10 March 2018).

Upward, F. 1996. Structuring the records continuum part one: post-custodial principles and properties. *Archives and Manuscripts*, 24(2): 268-285.

Upward, F. 1997. "Structuring the records continuum – part two: structuration theory and recordkeeping". Archives and Manuscripts. 25 (1): 10–35.

Upward, F. 2000. Modeling the continuum as paradigm shift in recordkeeping and archiving processes and beyond- a personal reflection. *Records Management Journal*, 10 (3):115-139.

Upward, F. 2004. Modeling the continuum as paradigm shift in recordkeeping and archiving processes and beyond-a personal reflection. *Records management journal*, 10 (3):116-139.

US Department of Commerce, National Institute of Standards and Technology NIST computer security information center, 2018. Role-based access control. [online]Available at: https://csrc.nist.gov/projects/role-based-access-control (accessed October 11 2018).

US Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-124., 2013. Guidelines for managing the security of Mobile devices in enterprise. [online]Available at: https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final (accessed October 11 2018).

US Department of Commerce, National Institute of Standards and Technology (NIST) Special Publication 800-46., 2016. Guidelines to the enterprise telework remote access and BYOD security. [online]Available at: https://csrc.nist.gov/publications/detail/sp/800-46/rev-2/final (accessed October 11, 2018).

US Department of Defence (DOD) 5015, 2007. *Design criteria standard for electronic records management software applications*. Department of Defense.

US Department of Defense (DoD) 5015.2, 2007. *Electronic records management software applications design criteria standard for electronic records management software applications*. Department of Defense.

Venkatesh, V., Davi, G.B. and Davis, F.D. 2013. User acceptance of information technology: Towards a unified view (PDF). *MIS Quarterly*, 27 (3): 425-478.

Virginia University 2017. Data protection of university information. [online] Available at: http://security.virginia.edu/ (accessed 6 June 2018).

Virginia University 2017. Device security guidance. [online]Available at: http://its.virginia.edu./accounts/passwords.html(accessed 6 June 2018).

Wamukoya, J. 2009. Public sector information management in East and Southern Africa: Implication for democracy and governance. *East African journal of information sciences*, 1(2): 67-87

Wamukoya, J. 2013. The role of recordkeeping and open government: Data initiatives in fostering a critical development of open government policies. *Mousion*, 30 (2):116-126.

Wamukoya, J. and Mutula, S.M. 2005. Opinion Piece. Capacity Building Requirements for E-records Management: The Case in East and Southern Africa. *Records Management Journal*, 15 (2):71-93.

Wamukoya, J. and Mutula, S.M. 2005b. E-Records Management and Governance in East and Southern Africa. *Malaysian Journal of Library and Information Science*, 10 (2): 67-83.

Water information sharing and analysis center (US, Canada, and Australia WaterISAC) 2016. 10 basic cybersecurity measures: best practices to reduce exploitable weaknesses and attacks. [online]Available at: https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_Oct2016%5B2%5D.pdf (accessed September 2018).

White House, 2011. Presidential memorandum -Managing government records. Memorandum for the heads of executive department and agencies. [online]Available at: https://obamawhitehouse.archives.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records (accessed 13 October 2017).

Williams, W. 2013. Records and archives: concepts, roles and definitions in archives and record-keeping. In C., Brown Ed. *Theory into practice*, pp1-29. London, Facet Publishing.

Willis, A. 2005. Corporate governance and management of information and records. *Records Management of information journal*, 15(2): 86-97.

Wood K., and Brown G., 2010. Assisted emulation for legacy executables. *International Journal of Digital Curation*,. 5 (1):153-216.

World Anti-Doping Agency (WADA), 2016. Cybersecurity update: WADA's incident response. [online]Available at: https://www.wada-ama.org/en/media/news/2016-10/cyber-security-update-wadas-incident-response *(*accessed 2 September 2018).

World Bank, 2002. New-economy sector study: electronic government and governance: -Lessons for Argentina (English). [online]Available at: http://documents.worldbank.org/curated/en/527061468769894044/New-economy-sector-study-Electronic-government-and-governance-lessons-from-Argentina (accessed 2 October 2017).

Wu, X., (2009). Security architecture for sensitive information system. Ph.D. Thesis. Australia. Monash University.

Xiaomi A., 2009. The electronic records management in E-government strategy: Case studies and implication. Proceedings, 2009 international conference on networking and digital society. Guiyang Guizhou, China 30-31 May 2009, IEEE computer society conference publishing services.

Xiaomi, A. 2003. An Integrated Approach to Records Management. *The information management journal*, 37(4): 24-30.

Xiaomi, A. 2001. A Chinese view of records continuum methodology and implications for managing electronic records. Paper presented at an international symposium on the management of archival electronic records, Theory and Practice. Hanghou, China 11.

Yacoob, R.A. and Sabai, M.R. 2011. Electronic records management in Malaysia: a case in one government agency. Asia Pacific conference library & information education & practice.

Yeo, G. 2011. Rising to the level of a record? Some thoughts on records and documents. *Records management journal*, 21(1): 8-27.

Yin, R. 2009. *Case study research: design and methods.* 4th ed. Thousand Oaks, sage.

Yorkland Controls Ltd. 2007. Security access control basics. [online] Available at: https://www.yumpu.com/en/document/view/30277170/security-access-control-basics-pdf-yorkland-controls (accessed 15 May 2018).

Yusof, Z.M. and Chell, W.R. 2000. The records life cycle: an inadequate concept for technology-generated records. *Information development,* 16(3): 135-141.

Zach, L. and Peri, F.M. 2010. Practices for college and University Electronic records management (ERM) Programs: Then and Now. *The American Archivist*,73(1): 105-128.

APPENDICES

Appendix 1: Survey questionnaire for action and records officers at Moi University

Dear Respondent**,**

I kindly invite you to participate in the study entitled “**E-records security management at Moi University, Kenya**." The study covers electronic management practices, electronic records security practices, security classification, access controls, classification schemes, measures to ensure confidentiality, integrity, availability, authenticity, possession or control and utility of e-records, skills, and competencies, threats to e-records security and strategies for sound e-records security management.

This study is undertaken as part of the requirements for the fulfilment of the Ph.D. degree in information studies at the University of KwaZulu-Natal.

I will be grateful for you to assist me in this endeavor by responding to the questions below to the best of your knowledge. The questionnaire will take approximately 20 minutes. Please note that your responses will be treated in confidence and will not be used for any other purposes. Thank you for participating in this research project.

Section A: BIODATA OF RESPONDENTS

Department: ________________________________

Designation: ________________________________

Gender: Male [ ] Female [ ]

Age category: 20-30 years [ ] 30-40 years [ ] 40-50 years [ ] 50-60 years [ ] above 60 years [ ]

Highest level of educational attainment

Certificate [ ] Diploma [ ] Undergraduate degree [ ] Master’s Degree [ ] PhD [ ] other [ ] Specify..................

For how long have you worked at Moi University in your current position?

0 - 2 years [ ] 3 - 6 years [ ] Over 10 years [ ]

How many staff are you managing under your current position?

None [ ] 1-10 [ ] 11 -20 [ ] 21-30 [ ] 31-40 [ ] more than 41

Describe your duties in the current position at Moi University

…………………………………………………………………………………………
……………………………………………………………………………………

Part B: e-Records Creation, Maintenance, Storage, Preservation, and Disposal

1. E-records creation

   a) What are the functions of your department that are pertinent to records management?

   ....
   ....
   ....

   b) Outline the types of records that are created and the people who create them at Moi University?

   ....
   ....
   ....

   c) What are standard formats available for e-records creation and capture?

   ....
   ....
   ....

   d) What standard procedure (if any) do you have in place for labeling storage devices such as computer disks?

....

....

....

e) How are e-records created by different departments at Moi University integrated and accessed?

....

....

....

2. Records maintenance and storage

a) Please explain how the e-records in your department are maintained?

....

....

....

b) Please outline how e-records are stored and subsequently handled in order to protect them from unauthorized access, loss, destruction theft and disaster at Moi University?

....

....

....

c) What designated areas are available for the storage of active, semi-active and non-active e-records?

....

....

....

d) What measures exist to ensure e-records remain accessible, authentic, reliable and usable through any system change during their retention?

....

....

....

3. **Appraisal and disposal**

a) At what stage are e-records appraised at Moi University?

....

....

....

b) What criteria do you use to appraise e-records at Moi University?

....

....

....

c) Please the guidelines if any for the retention and disposal of e-records.

....

....

....

d) Explain if Moi University has a structured disposal programme and what it entails

....

....

....

e) How do you ensure security at the disposal stage of e-records?

....

....

....

f) In your opinion, explain how the retention and disposal schedule tool is useful in the management of e-records

....

....

....

4. **Records preservation**

What strategies are used for the preservation of e-records at Moi University?

....

....

....

5. Please explain your knowledge about activities that are involved in administration and management of e-records throughout their lifecycle from creation to disposal.

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………………

……………………………………………………………………

6. Kindly, share how you ensure integration of e-recordkeeping functionalities into the universities business process

…………………………………………………………………………………………

…………………………………………………………………………………………

……………………………………………………………………………………

7. What policies, guidelines or regulations support e-records management at Moi University?

…………………………………………………………………………………………

…………………………………………………………………………………………

………………………………………………………………………………………

8. How effective are the existing e-records management policies, guidelines, and regulations (if any) at Moi University?

Adequate [ ]

Inadequate [ ]

9. Explain the extent to which records management is encapsulated in the vision, mission or strategic plan of Moi University

   ……………………………………………………………………………………………………
   ……………………………………………………………………………………………………
   ………………………………………………………………………………………………

10. To what extent do the available management systems meet all the e-records management functionalities at Moi University?

    ……………………………………………………………………………………………………
    ……………………………………………………………………………………………………
    …………………………………………………………………………………….

11. Please provide your opinion on the following statement about e-records management policies and regulations at Moi University

Key: 1 - strongly disagree, **2** - disagree, **3 -** undecided, **4 -** agree and **5 -** strongly agree

Assertions	**5**	**4**	**3**	**2**	**1**
The available policies and regulatory frameworks are adequate for the e-records security management					
Lack of policies and regulatory frameworks have led to poor e-records security management					
The available e-records policies and regulatory frameworks have been communicated at all levels of the University					
The university management is on the forefront in promoting the application of records management policies throughout the University					
The available policies and regulatory frameworks have enabled records to be maintained in a safe and secure environment					

<u>Part B:</u> Security classification of e-records process handling to facilitate description, Access control

19 To what extent do you agree with following assertions about e-records practices at Moi University

Key: 1 - strongly disagree, **2** - disagree, **3 -** undecided, **4 -** agree and **5 -** strongly agree

Assertions	**5**	**4**	**3**	**2**	**1**
The University's e-records security practices make it stand out among other institutions					
Availability of adequate policies and regulations framework support sound e-records security					
The University's achievements in its operations can be attributed to its e-records security practices					
Threat management and assessment carried out in the university is attributed to the security of records in the					
The access control mechanisms and safekeeping of passwords have enhanced the security of e-records					

12. Please indicate which of the following e-records security initiatives are available at Moi University

Statements	Available	Not available
E-records security Training programmes		
Monitoring access control to information and computing system by use of passwords, encryption, e.t.c.		

Frequent backing up of e-records		
Threat management and assessment programmes		
Security and access classification of e-record for instance, top secret, secret, sensitive, classified, confidential		
E- records security management policy		
Monitoring and auditing e-records protocol		
Physical control and monitoring of workplace environment and computing facilities		

13. Please state if you are aware of e-records security classification and level of access at Moi University?

    Yes [ ] No [ ]

14. If yes, what security classification is available at Moi University?

……………………………………………………………………………………………………
……………………………………………………………………………………………………
………………………………………………………………………………………

15. Please rate the following statement based on your level of agreement

    Key: 1 - strongly disagree, **2** - disagree, **3 -** undecided, **4 -** agree and **5 -** strongly agree

Assertions	**5**	**4**	**3**	**2**	**1**
Confidentiality and integrity of e-records is maintained at Moi University					

The university has provided clear guidelines to staff members to help determine which e-records need to be retained and preserved					
Security classification of e-records is aligned with the business functions					
e-records management is subjected to internal and external audit					
The University has ensured that there are clear procedures for planning, controlling, organizing, storing, maintaining, accessing, and disposing of e-records					
All staff in departments, project teams, and committees have been trained and sensitized on their role in managing e-records as they engage in their official daily work					

<u>Part C:</u> **Security Threats Predisposing E-Records to Damage, Destruction or Misuse**

16. Please state the types of e-records management threats the university faces on a regular basis in the course of carrying out its activities?

…………………………………………………………………………………………

…………………………………………………………………………………………

…………………………………………………………………………………

17. How often does the university carry out a threat assessment program?

Once per semester [ ]

Twice per semester [ ]

Annually [ ]

Biannually [ ]

Never [ ]

18. Assess the extent to which the tabulated challenges affect the security and management of e-records

Key: 1 - strongly disagree, **2** - disagree, **3 -** undecided, **4 -** agree and **5 -** strongly agree

Assertions	**5**	**4**	**3**	**2**	**1**
Inadequate policies and regulatory frameworks in records management and security					
Lack of training and skilled manpower in ICT and records management					
Ignorance of staff and low profile is given to records					
Lack of access control mechanisms and safe-keeping of passwords					
Inadequate regulations on defining and assigning e-records security management responsibilities					
Lack of access control and tracking of e-records					
Inadequate strategies in preserving e-records					
Assuming that any information online is safe					
Lack of disposal and retention schedules					
Others					

20 Please select from the list below the e-records preservation challenges experienced at Moi University?

Hackers and crackers [ ]

Technological obsolescence [ ]

Attacks from viruses [ ]

Loss and destruction of e-records [ ]

Mishandling of e-records [ ]

Environmental conditions [ ]

21 What strategies are used to overcome the above challenges?

....

....

....

22 State in your opinion, the critical success factors in e-records security at Moi University.

<u>Part D:</u> Measures to Protect Unauthorized Access to E-Records

23 What measures are available to e-records protection?

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………

24 How are the physical security of the premises, ICT infrastructure, computers and laptops ensured at Moi University?

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………

25 Please, what measures are available to protect your intranet against external and internal cyber attacks

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………

26 How often (if applicable) do you carry out self-evaluation and review of e-records security management practices at Moi University?

…………………………………………………………………………………………………

…………………………………………………………………………………………………

………………………………………………………………………………………

Part E: Confidentiality, Integrity, Availability, Authenticity, Control, and Utility of E-Records

27 State whether or not the following e-records security ethical values have been achieved at Moi University?

Ethical values	**Achieved**	**Not achieved**
Confidentiality of e-records		
Availability of e-records		
Integrity of e-records		
Authenticity of e-records		
Possession/control of e-records		
Utility of e-records		
Accessibility of records		

Part F: Skills and Competencies of E-Records at Moi University

28 What training programmes in e-records management are available to staff at Moi University?

………………………………………………………………………………………………

………………………………………………………………………………………………

……………………………………………………………………………………

29 How is awareness created among staff about e-records security at Moi University?

………………………………………………………………………………………………

………………………………………………………………………………………………

……………………………………………………………………………………

30 How often does the university organize conferences, workshops/seminars and public lecturers on e-records security?

Once per semester [ ]

Twice per semester [ ]

Annually [ ]

Biannually [ ]

Never [ ]

31 Does Moi University have training policy for records and if so what does it entail?

Appendix 2: Interview schedule for Top Management (Vice Chancellor & Deputy Vice Chancellors, Legal Officer) at Moi University

Dear Respondent**,**

I kindly invite you to participate in the study entitled "**E-records security management at Moi University, Kenya**." The study covers electronic management practices, electronic records security practices, security classification, access controls, classification schemes, measures to ensure confidentiality, integrity, availability, authenticity, possession or control and utility of e-records, skills, and competencies, threats to e-records security and strategies for sound e-records security management.

This study is undertaken as part of the requirements for the fulfilment of the Ph.D. degree in Information Studies at the University of KwaZulu-Natal, South Africa.

I will be grateful for you to assist me in this endeavor by responding to the questions to the best of your knowledge. The interview will take approximately 45 minutes. Please note that your responses will be treated in confidence and will not be used for any other purposes. Thank you for participating in this research project.

SECTION A: BIODATA OF RESPONDENTS

Department:________________________________

Designation: _________________________________

Date of interview:_____________________________

Gender: Male [ ] Female [ ]

Age category: 20-30 years [ ] 30-40 years [ ] 40-50 years [ ] 50-60 years [ ] above 60 years [ ]

Highest level of educational attainment

Certificate [ ] Diploma [ ] Undergraduate degree [ ] Masters Degree [ ] PhD [ ] other [ ] Specify..................

For how long have you worked in your current position at Moi University?

0 - 2 years [ ] 3 - 6 years [ ] 7-10 years [ ] Over 10 years [ ]

How many staff are you managing under your current position? --------------------

Describe your duties in your current position at Moi University -------------------------------

----

SECTION B:

Part A: E-Records Creation, Maintenance, Storage, Preservation and Disposal

1. Please explain how e-records are created, maintained, stored, preserved and disposed, at Moi University
2. Please explain your role in the records lifecycle from creation to disposal in your position at Moi University
3. Please explain to us the University's vision and scope of records management in providing strategic direction
4. Kindly, how does e-records management affect the implementation of ISO 9001:2008 at Moi University?
5. What is the University's vision and scope of e-records management in enhancing good governance and business practices
6. Please explain how you ensure integration of e-recordkeeping functionalities into the universities business process
7. What institutional policy and regulatory framework are used to guide e-records security management at Moi University?

Part B: Security classification of e-records process handling to facilitate description, Access control

8. How is e-records security practiced and managed at Moi University?
9. Kindly, what is the proportion of the institution budget that is allocated to e-records management including security?
10. Kindly explain the infrastructure that is available for e-records security management at Moi University
11. What is the place of e-records security management in the organization structure at Moi University?
12. To what extent is e-records management security integrated into the current strategic plan of Moi University?
13. What e-records security plans have been identified for the next five years?
14. Does the policy if available impose security classification or any other restrictions on some of the records?
15. How are business activities and security access classification on e-records management aligned?
16. Please explain how security classification of e-records process is handled to facilitate description, control, link and determination of disposal and access status
17. How does the university user permission register if any distinguish user permission to authorize, access, alter, or delete records maintained in e-records system to enhance the e-records security ethical values?
18. What does records access policy at Moi University entail if available?

Part C: Security Threats Predisposing E-Records to Damage, Destruction or Misuse

19. Please explain the issues that guide you during threat assessment in the University?

20. Please outline any security threats that predispose e-records to damage, destruction or misuse at Moi University and how are these ameliorated?

Part D: Measures to Protect Unauthorized Access to E-Records

21. Please, what set of responsibilities and practices are exercised to protect unauthorized access to e-records?

22. Please, what measures are available to protect your intranet against external and internal cyber attacks

23. What backup measures including offsite storage and insurance are available to ensure security of e-records at Moi University**?**

24. Briefly describe the state of physical security infrastructure available to protect e-records in the university;

25. Please state to us the disaster planning and recovery measures available in Moi University

Part E: Confidentiality, Integrity, Availability, Authenticity, Control, and Utility of E-Records at Moi University

26. Please share with us how the following e-records security ethical values of confidentiality, integrity, availability, authenticity, possession or control, accessibility, and utility of e-records are achieved at Moi University

Part F: Skills and Competencies of E-Records Management at Moi University

27. Outline skills you look for when recruiting records management staff

28. What is the level of academic and professional qualification required for record staff at Moi University?

29. How adequate are records officers in staff sufficiency and qualification?

30. How are records and action officers incentivized in their work?

31. What training policy for records and action officers does Moi University have in place?

32. Are the human resources and capacity building programmes available to ensure effective e-records security management adequate?

Appendix 3: Interview schedule for deans of schools and directors of centers

Dear Respondent**,**

I kindly invite you to participate in the study entitled "**E-records security management at Moi University, Kenya**." The study covers electronic management practices, electronic records security practices, security classification, access controls, classification schemes, measures to ensure confidentiality, integrity, availability, authenticity, possession or control and utility of e-records, skills, and competencies, threats to e-records security and strategies for sound e-records security management.

This study is undertaken as part of the requirements for the fulfilment of the Ph.D. degree in Information Studies at the University of KwaZulu-Natal, South Africa.

I will be grateful for you to assist me in this endeavor by responding to the questions to the best of your knowledge. The interview will take approximately 45 minutes. Please note that your responses will be treated in confidence and will not be used for any other purposes. Thank you for participating in this research project.

SECTION A: BIODATA OF RESPONDENTS

Department________________________________

Designation: ________________________________

Date of interview_____________________________

Gender: Male [ ] Female [ ]

Age category: 20-30 years [ ] 30-40 years [ ] 40-50 years [ ] 50-60 years [ ] above 60 years [ ]

Highest level of educational attainment

Certificate [ ] Diploma [ ] Undergraduate degree [ ] Master's Degree [ ] Ph.D. [ ] others [ ] Specify..................

For how long have you worked at Moi University in your current position?

0 - 2 years [ ] 3 - 6 years [ ] 7-10 years { } Over 10 years [ ]

Please state the number of staff you are managing in your current portfolio?

What is the scope of your duties in your current position? --
----

SECTION B: QUESTIONS

Part A: E-Records Creation, Maintenance, Storage, Preservation and Disposal

1. Management of e-records throughout their lifecycle is critical to any organization. Please explain how e-records are created, maintained, stored, preserved and disposed at Moi University

2. Please explain your role in the records lifecycle from creation to disposal in your current position at Moi University

3. To achieve best practice and uniformity in the e-records security management, please share with us which standards are adhered to at Moi University?

4. Please explain the institutional policy and regulatory framework that is used to guide e-records security management at Moi University
5. Recordkeeping function must be integrated into the business process of any organization to enhance governance. Please outline how integration of e-recordkeeping functionalities into the universities business process is ensured at Moi University

Part B: Security classification of e-records process handling to facilitate description, Access control

6. Records security is an elusive function of recordkeeping. Please explain how e-records security is practiced and managed at Moi University
7. To what extent is the e-records security management subject to any external audit?

8. Internal mechanisms for e-records review and evaluation are useful to ensure sound records management practices. Please tell us how self-evaluation and review of e-records management of e-records is undertaken

9. To carry out sound e-records activities, a comprehensive budget is vital. How adequate and comprehensive is e-records security budgets in the University

10. Classification of business activities acts as a tool to assist the conduct of business and in many of the processes involved in the management of e-records. Discuss your role in business activity analysis at Moi University

11. Records classification ensures continued access to records over time. Kindly explain how security classification of e-records process is handled to facilitate description, control, link and determination of disposal and access status?

12. Regulatory framework establishes broad principles on access rights. What mechanism including policies does Moi University apply to enhance e-records access?

13. Please, what restrictions are imposed upon security classification or any other restrictions on some of the e-records?

Part C: **Security Threats Predisposing E-Records to Damage, Destruction or Misuse**

14. Many security threats exist in organization that may compromise sound e-records management. Please outline any security threats that predispose e-records to damage, destruction or misuse at Moi University and how they are ameliorated

Part D: Measures to Protect Unauthorized Access to E-Records

15. Protection of business records of an organization is important to enhance its competitive advantage. What measures are in place to protect unauthorized access to e-records of your organization?
16. Records access must be restricted to enhance the integrity and security of the records. What security measures are available to ensure access to e-records is limited to authorized personnel only?
17. Quality assurance is an important component of records management. How does your directorate/school ensure quality control in security of e-records?

Part E: Confidentiality, Integrity, Availability, Authenticity, Control, and Utility of E-Records at Moi University

18. Ethical values in records management are vital tools for accountability purposes. Share your knowledge of how confidentiality, integrity, availability, authenticity, control, accessibility and utility of e-records is achieved at Moi University

19. Vetting is an important aspect to identify e-records staff background and circumstances. Please share with us if this process is done to meet the ethical values of e-records security management.

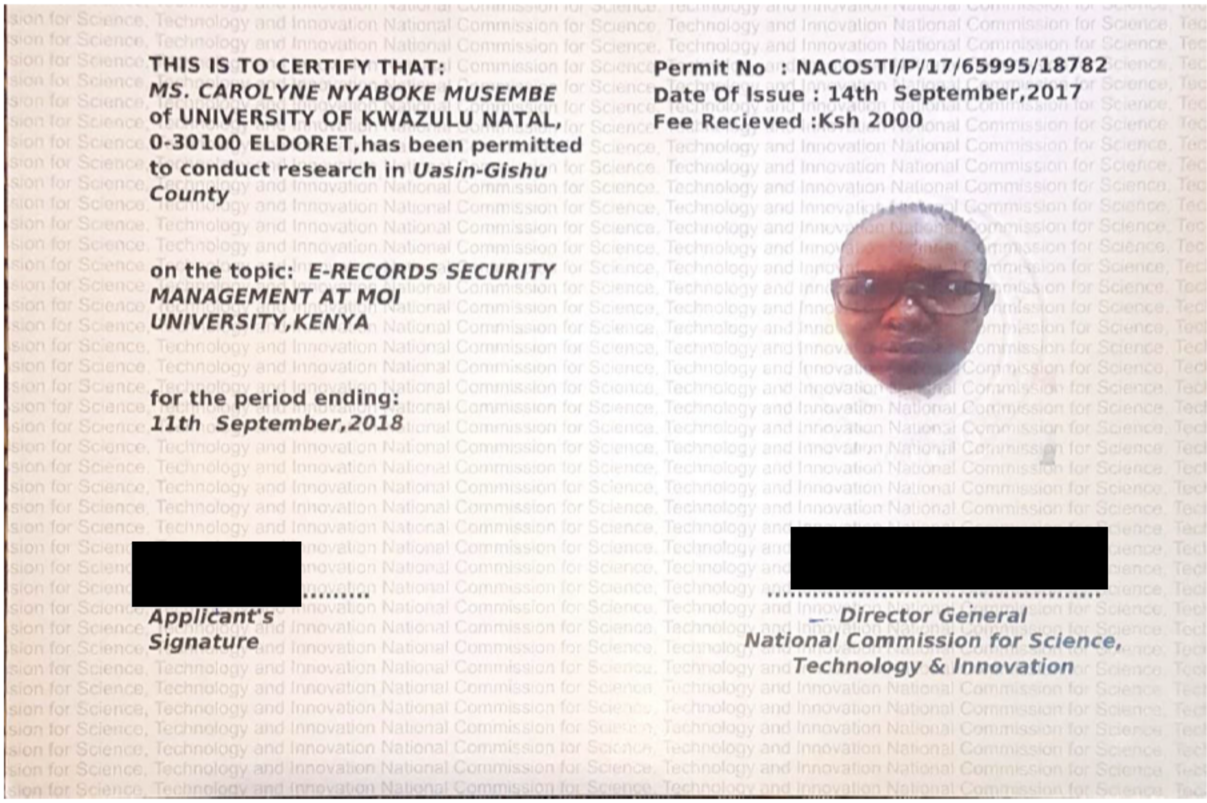
Part F: Skills and Competencies of E-Records at Moi University

20. What competencies and skills of records and action officers are available for e-records management at Moi University?

21. How do you ensure staff retention and succession plans at Moi University?

22. Capacity building and continuous education and training are important activities in records management. How do you ensure training and continuing education of records and action officers?

Appendix 4: NACOSTI Permit



THIS IS TO CERTIFY THAT:
MS. CAROLYNE NYABOKE MUSEMBE
of UNIVERSITY OF KWAZULU NATAL,
0-30100 ELDORET,has been permitted
to conduct research in *Uasin-Gishu County*

on the topic: ***E-RECORDS SECURITY MANAGEMENT AT MOI UNIVERSITY,KENYA***

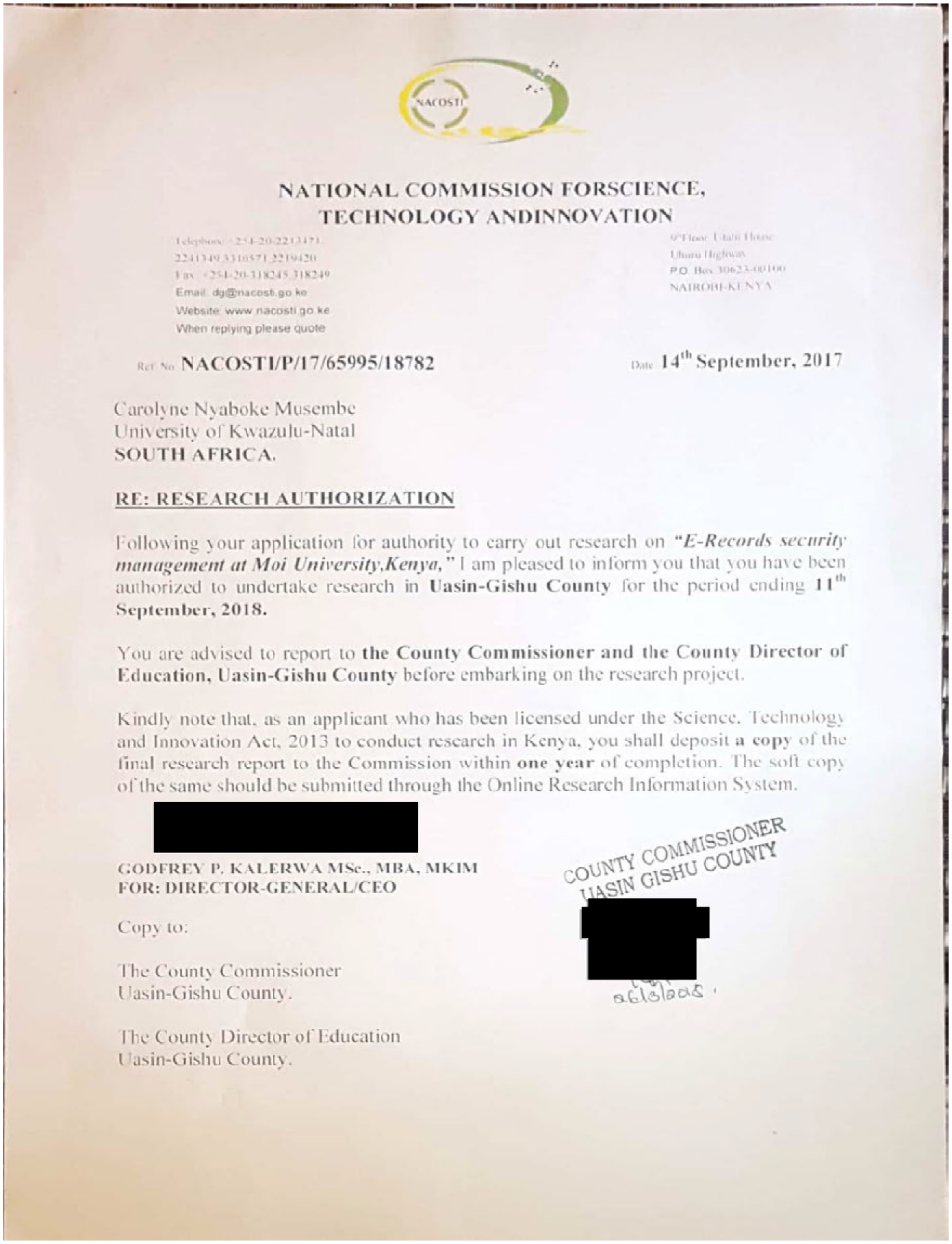
for the period ending:
11th September,2018

Permit No : NACOSTI/P/17/65995/18782
Date Of Issue : 14th September,2017
Fee Recieved :Ksh 2000

[redacted]........
Applicant's Signature

[redacted]
Director General
National Commission for Science, Technology & Innovation

Appendix 5: Clearance letter from NACOSTI and approval stamp from County Commissioner Uasin-Gishu County



NACOSTI

NATIONAL COMMISSION FORSCIENCE, TECHNOLOGY ANDINNOVATION

Telephone +254-20-2213471,
2241349,3310571,2219420
Fax +254-20-318245,318249
Email: dg@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

9thFloor Utalii House
Uhuru Highway
P.O. Box 30623-00100
NAIROBI-KENYA

Ref No. **NACOSTI/P/17/65995/18782**

Date **14th September, 2017**

Carolyne Nyaboke Musembe
University of Kwazulu-Natal
SOUTH AFRICA.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"E-Records security management at Moi University,Kenya,"*** I am pleased to inform you that you have been authorized to undertake research in **Uasin-Gishu County** for the period ending **11th September, 2018.**

You are advised to report to **the County Commissioner and the County Director of Education, Uasin-Gishu County** before embarking on the research project.

Kindly note that, as an applicant who has been licensed under the Science, Technology and Innovation Act, 2013 to conduct research in Kenya, you shall deposit **a copy** of the final research report to the Commission within **one year** of completion. The soft copy of the same should be submitted through the Online Research Information System.

[redacted]

GODFREY P. KALERWA MSc., MBA, MKIM
FOR: DIRECTOR-GENERAL/CEO

COUNTY COMMISSIONER
UASIN GISHU COUNTY

[redacted]

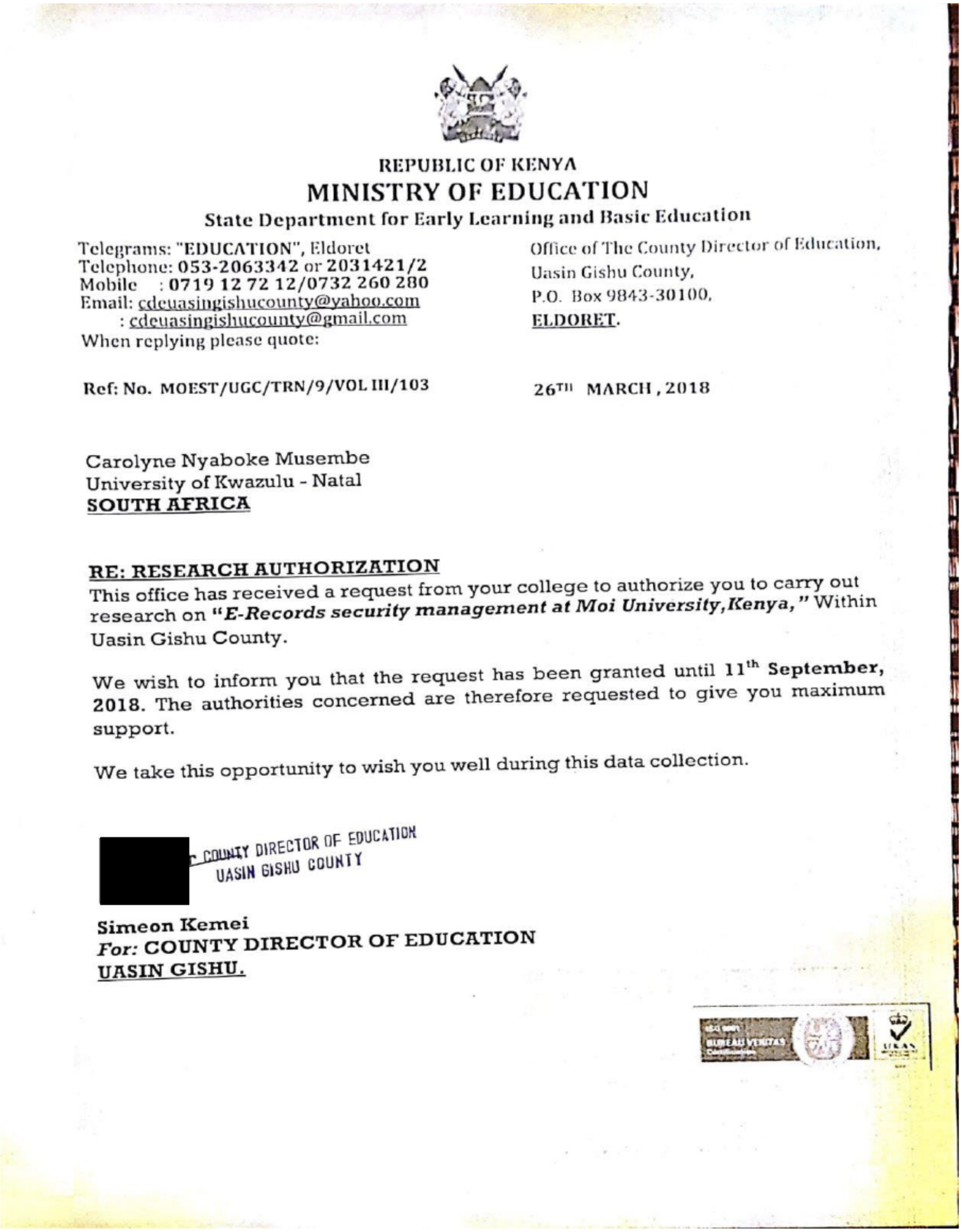
26/3/2018

Copy to:

The County Commissioner
Uasin-Gishu County.

The County Director of Education
Uasin-Gishu County.

Appendix 6: Approval from County Commissioner of Education Uasin-Gishu County



REPUBLIC OF KENYA

MINISTRY OF EDUCATION

State Department for Early Learning and Basic Education

Telegrams: "EDUCATION", Eldoret
Telephone: 053-2063342 or 2031421/2
Mobile : 0719 12 72 12/0732 260 280
Email: cdeuasingishucounty@yahoo.com
: cdeuasingishucounty@gmail.com
When replying please quote:

Office of The County Director of Education,
Uasin Gishu County,
P.O. Box 9843-30100,
ELDORET.

Ref: No. MOEST/UGC/TRN/9/VOL III/103

26TH MARCH, 2018

Carolyne Nyaboke Musembe
University of Kwazulu - Natal
SOUTH AFRICA

RE: RESEARCH AUTHORIZATION

This office has received a request from your college to authorize you to carry out research on ***"E-Records security management at Moi University, Kenya,"*** Within Uasin Gishu County.

We wish to inform you that the request has been granted until **11th September, 2018.** The authorities concerned are therefore requested to give you maximum support.

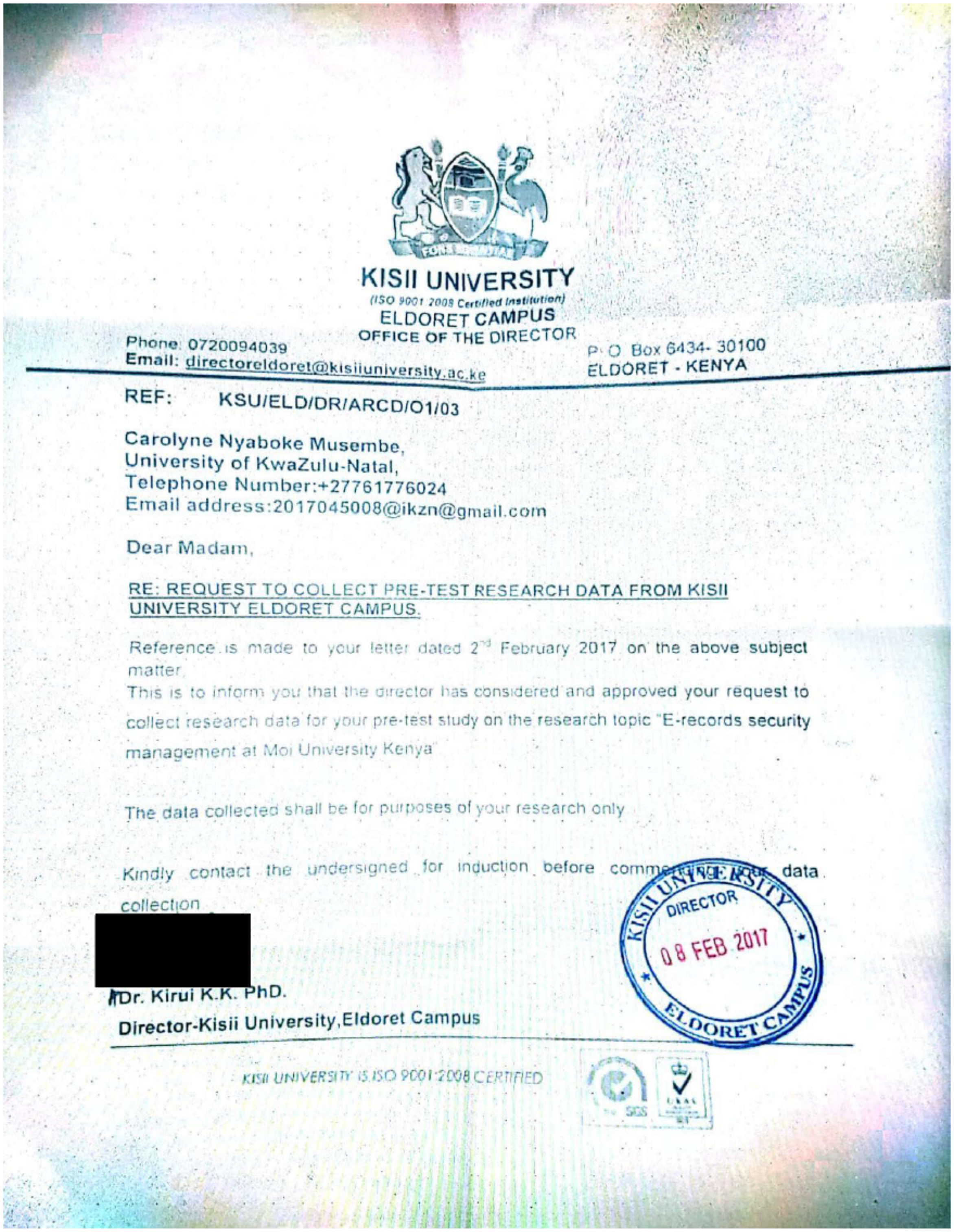
We take this opportunity to wish you well during this data collection.

[redacted]

COUNTY DIRECTOR OF EDUCATION
UASIN GISHU COUNTY

Simeon Kemei
For: **COUNTY DIRECTOR OF EDUCATION**
UASIN GISHU.

Appendix 7: Approval to carry out pre-test study



KISII UNIVERSITY
(ISO 9001 2008 Certified Institution)
ELDORET CAMPUS
OFFICE OF THE DIRECTOR

Phone: 0720094039
Email: directoreldoret@kisiiuniversity.ac.ke

P. O Box 6434- 30100
ELDORET - KENYA

REF: KSU/ELD/DR/ARCD/O1/03

Carolyne Nyaboke Musembe,
University of KwaZulu-Natal,
Telephone Number:+27761776024
Email address:2017045008@ikzn@gmail.com

Dear Madam,

RE: REQUEST TO COLLECT PRE-TEST RESEARCH DATA FROM KISII UNIVERSITY ELDORET CAMPUS.

Reference is made to your letter dated 2nd February 2017 on the above subject matter.

This is to inform you that the director has considered and approved your request to collect research data for your pre-test study on the research topic "E-records security management at Moi University Kenya"

The data collected shall be for purposes of your research only

Kindly contact the undersigned for induction before commencing your data collection

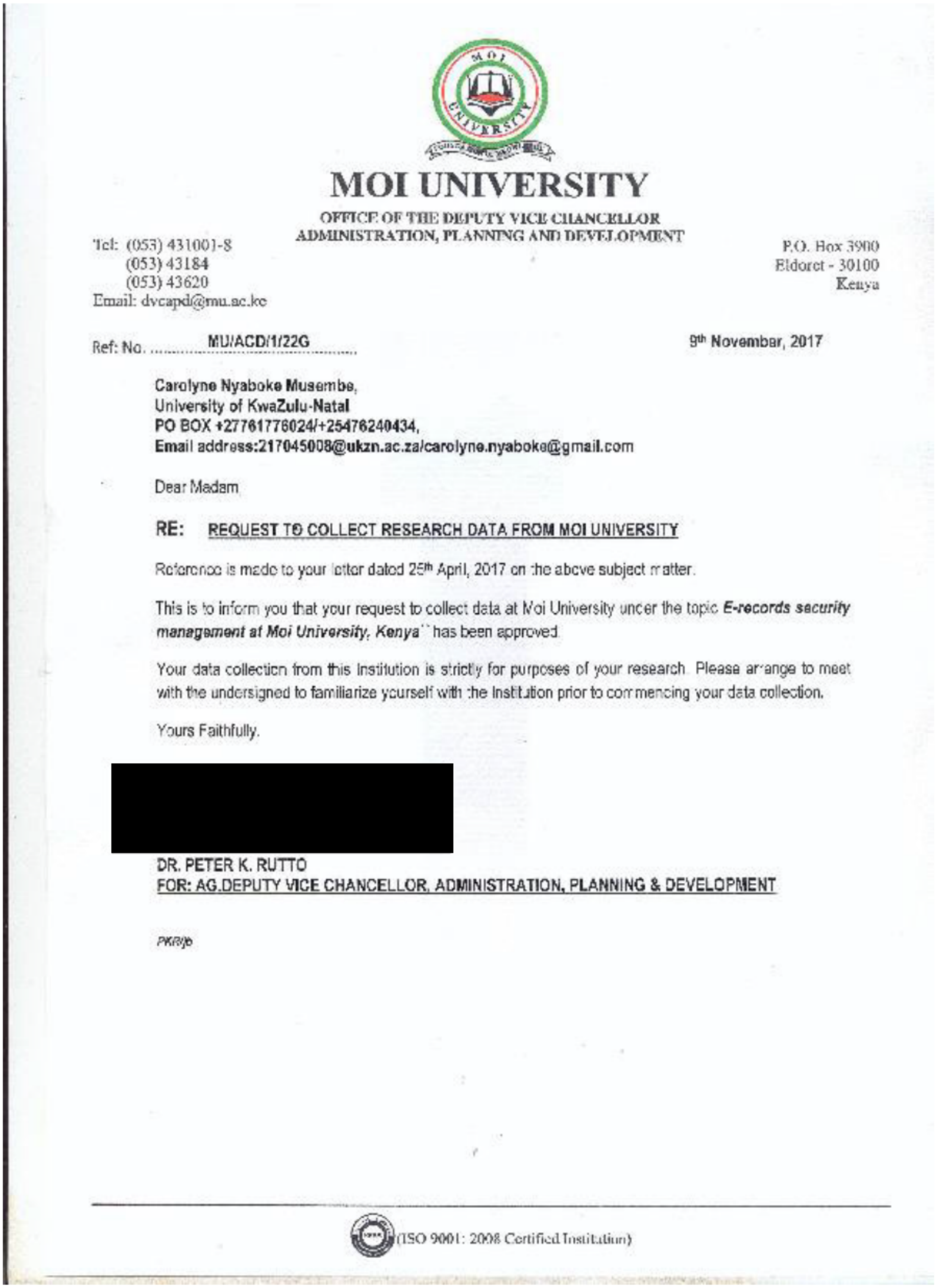
KISII UNIVERSITY
DIRECTOR
08 FEB 2017
ELDORET CAMPUS

[redacted]

Dr. Kirui K.K. PhD.
Director-Kisii University,Eldoret Campus

KISII UNIVERSITY IS ISO 9001:2008 CERTIFIED

Appendix 8: Permission to collect research data from Moi University



MOI UNIVERSITY

OFFICE OF THE DEPUTY VICE CHANCELLOR
ADMINISTRATION, PLANNING AND DEVELOPMENT

Tel: (053) 431001-8
(053) 43184
(053) 43620
Email: dvcapd@mu.ac.ke

P.O. Box 3900
Eldoret - 30100
Kenya

Ref: No. ....MU/ACD/1/22G............

9th November, 2017

Carolyne Nyaboke Musembe,
University of KwaZulu-Natal
PO BOX +27761776024/+25476240434,
Email address:217045008@ukzn.ac.za/carolyne.nyaboke@gmail.com

Dear Madam

RE: REQUEST TO COLLECT RESEARCH DATA FROM MOI UNIVERSITY

Reference is made to your letter dated 25th April, 2017 on the above subject matter.

This is to inform you that your request to collect data at Moi University under the topic ***E-records security management at Moi University, Kenya*``** has been approved.

Your data collection from this Institution is strictly for purposes of your research. Please arrange to meet with the undersigned to familiarize yourself with the Institution prior to commencing your data collection.

Yours Faithfully,

[redacted]

DR. PETER K. RUTTO
FOR: AG.DEPUTY VICE CHANCELLOR, ADMINISTRATION, PLANNING & DEVELOPMENT

PKR/jb

(ISO 9001: 2008 Certified Institution)

Appendix 9: Informed Consent Letter

Information Studies
School of Social Sciences
University of KwaZulu-Natal
Pietermaritzburg Campus
Private Bag X01
Scottsville
Telephone: +27761776024
Email: 217045008@ukzn.ac.za

9 November, 2017

Dear Respondent,

Informed Consent Letter

Researcher: Carolyne Nyaboke Musembe
Institution: University of KwaZulu-Natal
Email address: [redacted]

Supervisor: Prof. S. Mutula
Institution: University of KwaZulu-Natal
Telephone number: +27(0)33-260 5007
Email address: mutulas@ukzn.ac.za

I, Carolyne Nyaboke Musembe kindly invite you to participate in the research project entitled "**E-records security management at Moi University, Kenya."**

This research project is undertaken as part of the requirements of the Ph.D., which is undertaken through the University of KwaZulu-Natal, Information Studies Department.

The aim of this study is to investigate e-records security management at Moi University, Kenya and come up with strategies for improvement.

Participation in this research project is voluntary. You may withdraw from the research project at any stage and for any reason without any form of disadvantage. There will be no monetary gain from participating in this research project. Confidentiality and anonymity will be maintained by the by the researcher and also by the Information Studies Programme, at the University of KwaZulu-Natal.

If you have any questions or concerns about participating in this study, please feel free to contact myself or my supervisor at the numbers indicated above.

It should take you about 15 minutes to complete the questionnaire, and the interview will take approximately 1 hour.

Thank you for participating in this research project.

[redacted] 9th November 2017

---------------------- --------------------

Signature Date

I .... hereby consent to participate in the above study.

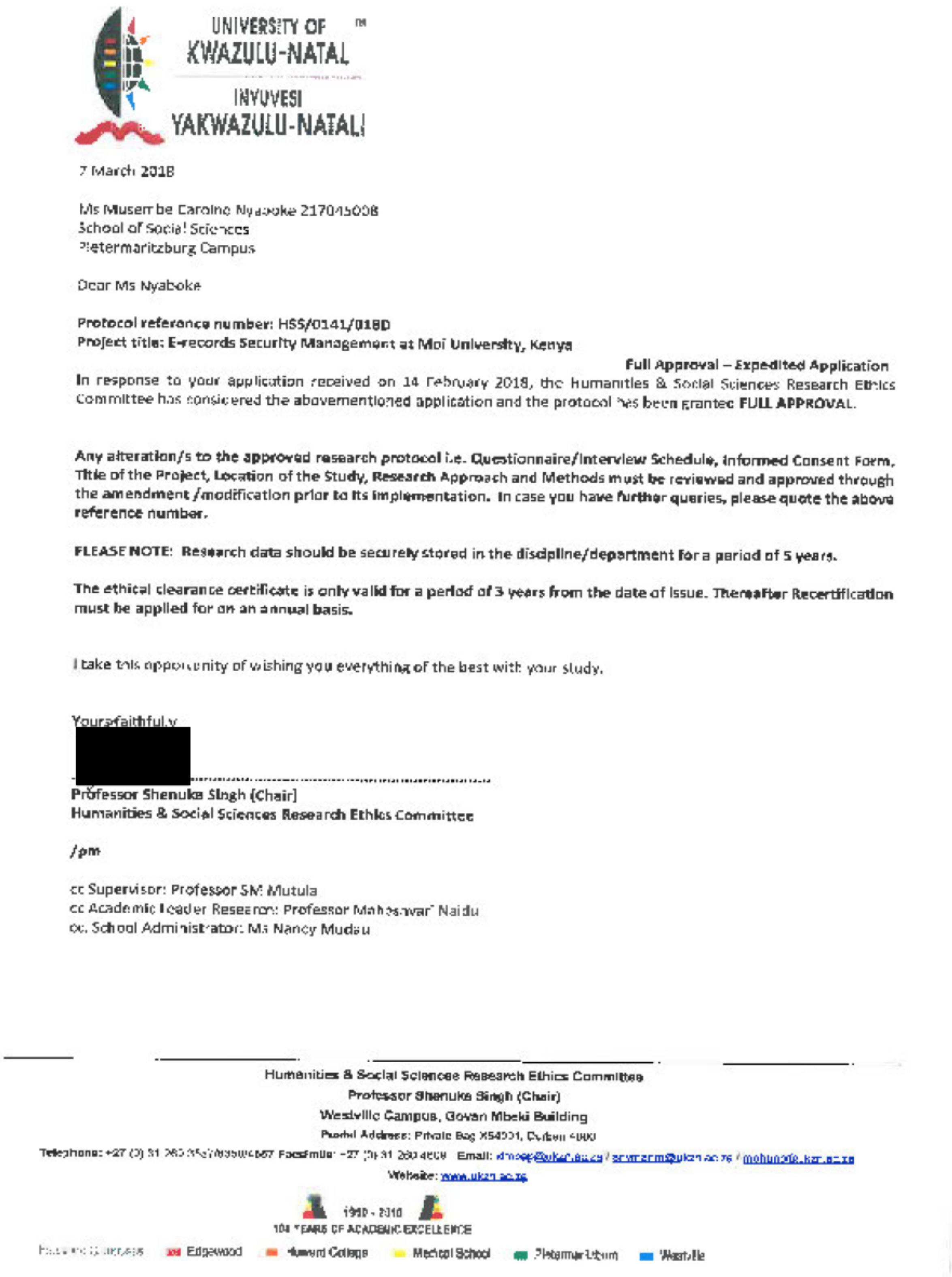
Name: .... Date: .... Signature: ....

Supervisor's details **Student's details**

Prof. S. Mutula
University of KwaZulu-Natal
Telephone number:+27(0)33-260 5007
Email address: mutulas@ukzn.ac.za

Carolyne Nyaboke Musembe
University of KwaZulu-Natal
Telephone number: [redacted]
Email: 217045008@ukzn.ac.za

Appendix 10: Ethical clearance from UKZN



UNIVERSITY OF KWAZULU-NATAL
INYUVESI YAKWAZULU-NATALI

7 March 2018

Ms Musembe Caroline Nyaboke 217045008
School of Social Sciences
Pietermaritzburg Campus

Dear Ms Nyaboke

Protocol reference number: HSS/0141/018D
Project title: E-records Security Management at Moi University, Kenya

Full Approval – Expedited Application

In response to your application received on 14 February 2018, the Humanities & Social Sciences Research Ethics Committee has considered the abovementioned application and the protocol has been granted **FULL APPROVAL**.

Any alteration/s to the approved research protocol i.e. Questionnaire/Interview Schedule, Informed Consent Form, Title of the Project, Location of the Study, Research Approach and Methods must be reviewed and approved through the amendment /modification prior to its implementation. In case you have further queries, please quote the above reference number.

PLEASE NOTE: Research data should be securely stored in the discipline/department for a period of 5 years.

The ethical clearance certificate is only valid for a period of 3 years from the date of issue. Thereafter Recertification must be applied for on an annual basis.

I take this opportunity of wishing you everything of the best with your study.

Yours faithfully

[redacted]

Professor Shenuka Singh (Chair)
Humanities & Social Sciences Research Ethics Committee

/pm

cc Supervisor: Professor SM Mutula
cc Academic Leader Research: Professor Maheshvari Naidu
cc. School Administrator: Ms Nancy Mudau

Humanities & Social Sciences Research Ethics Committee
Professor Shenuka Singh (Chair)
Westville Campus, Govan Mbeki Building
Postal Address: Private Bag X54001, Durban 4000
Telephone: +27 (0) 31 260 3587/8350/4557 Facsimile: +27 (0) 31 260 4609 Email: ximbap@ukzn.ac.za / snymanm@ukzn.ac.za / mohunp@ukzn.ac.za
Website: www.ukzn.ac.za

1910 - 2010
100 YEARS OF ACADEMIC EXCELLENCE

Founding Campuses 🟥 Edgewood 🟧 Howard College 🟨 Medical School 🟩 Pietermaritzburg 🟦 Westville

Appendix 11: Informed consent letter for interviews

Social Sciences, College of Humanities,
University of KwaZulu-Natal,
Pietermaritzburg Campus,

Dear Participant

INFORMED CONSENT LETTER

My name is Ms Musembe Carolyne Nyaboke, I am a PhD candidate studying at the University of KwaZulu-Natal, Pietermaritzburg campus, South Africa.

I am interested in learning about E-records security management at Moi University, Kenya. The aim of the study is to investigate e-records security management at Moi University, Kenya and come up with strategies for improvement. Your department forms my target group. To gather the information, I am interested in asking you some questions.

Please note that:

- Your confidentiality is guaranteed as your inputs will not be attributed to you in person, but reported only as a population member opinion.
- The interview may last for approximately 30 minutes and may be split depending on your preference.
- Any information given by you cannot be used against you, and the collected data will be used for purposes of this research only.
- Data will be stored in secure storage and destroyed after 5 years.
- You have a choice to participate, not participate or stop participating in the research. You will not be penalized for taking such an action.
- The research aims at knowing the challenges of your community relating to resource scarcity, peoples' movement, and effects on peace.
- Your involvement is purely for academic purposes only, and there are no financial benefits involved.
- If you are willing to be interviewed, please indicate (by ticking as applicable) whether or not you are willing to allow the interview to be recorded by the following equipment:

	willing	Not willing
Audio equipment		

I can be contacted at: Email: carolyne.nyaboke@gmail.com

My supervisor is Professor S Mutula who is located at the School of Social Sciences, Pietermaritzburg campus of the University of KwaZulu-Natal.
Contact details: email: mutulas@ukzn.ac.za   Phone number: 033 2605571

You may also contact the Research Office through:
P. Mohun
HSSREC Research Office,
Tel: 031 260 4557 E-mail: mohunp@ukzn.ac.za

Thank you for your contribution to this research.

DECLARATION

I…………………………………………………………………………… (Full names of

participant) hereby confirm that I understand the contents of this document and the nature of the research project, and I consent to participating in the research project.

I understand that I am at liberty to withdraw from the project at any time, should I so desire.

SIGNATURE OF PARTICIPANT   DATE

……………………………………..   …………………………………