Enhancing security ethical value practices in e-records management at Moi University, Eldoret, Kenya

Vol. 6 No. 2

October 2021

Dr. Carolyne Nyaboke Musembe
University of Kwa-Zulu Natal
carolyne.nyaboke@gmail.com

Prof. Stephen Mutula
University of Kwa-Zulu Natal
mutulas@ukzn.ac.za

Abstract

Rationale of Study – This paper, which is part of a doctoral thesis on e-records security management, investigates security ethical values in e-records management with a view to offering practical and policy interventions to address this challenge.

Methodology – Data was collected from Moi University staff in Kenya using interviews and questionnaires and analysed thematically using Statistical Package for Social Sciences (SPSS) Version 24.

Findings – The study revealed that security ethical values were practised to some extent in the university. However, with the decentralised nature of running the university affairs, especially in schools and departments, and lack of guiding principles coupled with weak implementation of classification of e-records, the security of the information was left at the mercy of individual staff. Similarly, the study found that the university lacks clear guidelines on the standard way of sensitising personnel on the security ethical values.

Implications **–** The university should consider the application of security ethical values considering the continuous development in technology by developing a robust set of principles to underpin new approaches in e-records management.

Originality – Security ethical values is an area with multidimensional complexities that invites intelligence of professionals in different fields and stakeholders that has not been broadly covered in literature. This paper tries to bring out fundamental principles that may contribute to the existing knowledge.

Published by the

Regional Institute of Information and Knowledge Management

P.O. Box 24358 – 00100 –
Nairobi, Kenya

Keywords

E-records, security, security ethical values, security attributes

Citation: Musembe, C.N. & Mutula, S. (2021). Enhancing security ethical value practices in e-records management at Moi University, Eldoret, Kenya. *Regional Journal of Information and Knowledge Management*, 6 (2),1-20.

1 Introduction

E-records management is the central nerve in the administration of organisations globally. Planning, developing and implementing the appropriate course of services mandates the organisation to strive in securing the e-records at, or even before, creation and throughout their life cycle, as well as the systems that created. This is particularly important in this era of digital revolution (Musembe, 2019). In November 28, 2011, President Barack Obama issued a memorandum on managing United States of America's government records. President Obama indicated that decades of technological advances had transformed agency operations thereby creating challenges and opportunities for agency records management. That greater reliance on electronic communication and systems has radically increased the volume and the diversity on the information that agencies must manage. The memorandum went on to point out that if records management policies and practices are not updated for the digital age, the surge in information could overwhelm agency systems leading to high cost and lost records (The White House, 2011).

Securing e-records, therefore, is a practice that organisations, both small and large, should devote utmost attention to and prioritise. Although, this has been practised since the early days where rulers and military entities sought new ways to secure their records by deterring and detecting records tampering, in recent times, and with the always advancing technology, securing e-records has become a major challenge which is becoming more complicated. As Bey (2012) asserts, 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 more difficult. 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.

This implies that security currently has changed meaning given the exponential advancement of the digital revolution. Perhaps, the attention of organisations should shift to the importance of being steady in adopting a variety of measures and strategies of securing records. This includes practising security ethical values and investing in the understanding of the cyberspace dynamics.

Some of the security challenges organisations are currently facing include, but not limited to, unauthorised information release, unauthorised information modification, unauthorised denial of use, and distributed denial of attacks, among others. However, with the global Internet connectivity enhanced by digital revolution as indicated earlier, the challenges have advanced. Kumar and Malhotra (2015) state that this has brought about the power to deface websites, access personal mail accounts, and worse more, the potential to bring down the entire government or institution through openly documented software codes.

Most organisations use extranets and intranets, both of which are private. An extranet is a private network that uses Internet protocols (IP), network connectivity and possibly the public communication system to securely share part of an organisation's electronic-records and other information or operations with suppliers, partners, customers or other business (it is extended to users outside the company). On the other hand, an intranet is a private network that uses IP, network connectivity and the public telecommunication system to securely share part of an organisation's e-records and other information or operations with its own 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, and also acts as a daily messaging channel to help drive the business effectively among employees, departments, and units worldwide (Musembe & Mutula, 2019).

Consequently, a network and system security architecture should be a tiered one and provide the ability to separate resources based on their e-records, business criticality and functions. Moreover, it ensures that appropriate controls exist within each level to address the threats and risks in the resources in a given tier thus enhancing security ethical values (University of Connecticut, 2011).

The security ethical values are described as values that uphold confidentiality, availability, integrity, authenticity, possession/control, authority, utility and non-repudiation in the management and use of records. They have been referred to by different authors as security attributes, features and even objectives (Bey, 2012; Parker, 1998). However, in many instances, the security ethical values in different studies have been inconsistently or interchangeably used. This should not be the case. The integrity, authenticity, confidentiality, control, and availability of e-records rest on the ability to demonstrate that the e-records have not been tampered with or accessed by unauthorised persons or documented software codes (security breach). They also rest on the assurance that they are accurate, relevant, consistent, timely, comprehensive and complete (Musembe & Mutula, 2019; Kabata, 2013). Therefore, e-records should be handled at all times as sensitive information that could have adverse effects if disclosed to unauthorised entities or parties. Organisations and institutions including Moi University's e-records have a strategic value to them and thus should be secured at all times. The records may include, but not limited to, records that hold financial information, human resources information, scientific formulas, and medical information, among others. Consequently, e-records security values rely heavily on the ability of personnel within a given organisation to perform their roles responsibly and with a clear understanding of how their integrity has a direct impact on the e-records they are charged with protecting. Chapple (2019) asserts that, in most cases, security breaches occur not as a result of a sophisticated technical failure but as a result of a mistake made by individuals with authorised access privileges to the e-records.

The aim of the study was to investigate security ethical value practices in e-records management in Moi University and come up with strategies for improvement. The specific objectives were to find out whether ethical values are applied and achieved at Moi University; and whether vetting of staff in meeting the security ethical values is carried out at the university.

2 Literature Review

E-records as well as system breaches have increased in the recent times. These breaches may refer to varied ways by which authorised or unauthorised people or programmes steal, share, delete, or temper with institutions' sensitive information such as email addresses, social security numbers, and bank account details, among others. Consequently, whether it is because of a lack of encryption, password cracking, careless privacy practices, and stealing of the devices, it can leave organisations vulnerable to lawsuits and serious breach issues.

Globally, universities that have experienced security breach incidences reveal vulnerabilities in information technology infrastructure (Pulseway, 2020). For instance, University of Greenwich in the United Kingdom was fined 16,000 USD by the Information Commission for a security breach in which personal data of 19,500 students was placed online (University of Greenwich, 2018; BBC, 2018). Washington State University also settled a lawsuit of 4.7million USD after a data breach. This was after a theft of portable hard-drives containing e-records of about 1.2 million people (Pulseway, 2020; Davis, 2019; Washington State University, 2019). In November 2018, Australian National University experienced a security breach on their systems where human resource records were affected (Australian National University, 2019; 2018; Groch, 2019; Pulseway, 2020).

In Africa, the Africa cybersecurity report (2018) indicated that loss to African businesses from cyber-crime was at 3.5 billion USD, up from 2 billion USD the previous year. Nigeria was the hardest hit with losses of 649 million USD, followed by Kenya with 210 million USD and Tanzania with 99 million USD. Meanwhile, more than 95% of public and private organisations across the continent spent less than 1,500 USD a year on cybersecurity measures, with SMEs in particular failing to invest. The Kenya Communication Authority indicated that cyber threats had risen by over 10% in the first quarter of 2019, which was attributed to the global increase in malwares that included ransomware attacks (Munyori & Mumbi, 2020).

In Ghana, the African University of Professional Studies also experienced a system breach where students' records were manipulated in 2017. Uganda's Makerere University's system was hacked and records deleted from a graduation list. In Kenya, the National Kenya Computer Incident Response Team Coordination Center reported that 26.6 million cyber-threats occurred between April and June 2019. However, clear reports on records and system breaches in universities is not well reported or not made public.

These system breaches affect the security ethical values (confidentiality, availability, integrity, authenticity, possession/control and utility) of the universities, governments, organisations and other institutions. The ethical values make a strong foundation and may solve the puzzle of comprehensive security of systems and the e-records. Notwithstanding the increased usefulness and increased enthusiasm to its adoption, not much attention is being paid to ethical issues that might arise.

Confidentiality is central to the creator and receiver of information and the organisation. Thus, they become accountable when confidentiality is breached. Confidentiality refers to the property that e-records is not made available or disclosed to unauthorised individuals, entities, or processes (Northeastern University, 2018; UNAIDS, 2016). This way of thinking is supported by the Parkerian Hexad Model which asserts that confidentiality is the limited observation and disclosure of knowledge (Parker, 2002).

Observing the integrity of e-records and systems that create and manage them is vital to an organisation for it ensures e-records remain accurate and unchanged representation of the original transaction (Bey, 2012; Parker, 2002). According to the Parkerian Hexad Model, integrity means information cannot be modified without authorisation (Parker, 2002). IRMT (2016) asserts that creating and protecting digital records and preserving their integrity are challenging for organisations and countries worldwide. The fragility of electronic media, the absence of accurate and complete metadata, and the rapid obsolescence of software and computer systems all place e-records at great risk of breach of integrity. For instance, the decision about upgrading software from one version to another or changing to another software altogether should not be made without considering the implication to the e-records and their on-going integrity. IRMT (2016) is of the opinion that while the challenges are the same everywhere, they can be particularly hard to address in lower resource environments, where the issues are just as complex as in well-resourced environments.

Many authors have asserted that availability is the most challenging component to protect though it has not been given extensive attention (Qadir & Quadri, 2016; Bey, 2012). Availability of e-records dictates reliability, accessibility and timeliness of e-records and the systems that hold them. In the digital era, cyberspace has brought with it a number of fortunes and misfortunes. Firstly, technologies have made availability to records easier and many activities and processes carried out in real time, thus enhancing decision making. However, the digital era has also compromised, to large extent, the availability component and in recent times they have increased in magnitude as many organisations embrace the digital technologies. Denial to access of available systems and e-records has costed organisations huge losses. This may be caused by denial-of-service attacks (DOS), and distributed denial of service attacks (DDOS), among others (Unites States of America Department of Homeland Security 2009).

Authenticity ensures the validity, trustworthiness, and dependability of e-records (Bey 2012; Antirion, 2011; Wu, 2009). It involves proof of identity (Clemmer, 2010). DoD 5015-2007 defines authenticity as a condition that proves that a record is genuine based on the mode (including method by which a record is communicated over space or time), form (format or media that a record has upon receipt), state of transmission (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; Ismail & Jamaludin, 2009).

Possession or control of e-records refers to the ownership or controlling the ability to use e-records (Musembe, 2019; Bey, 2012; Antirion, 2011). Parkerian Hexad Model defines possession or control as a state of having 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, laptops, IPads, Internet cafes, WiFi, as well as specialised and inexpensive Internet access devices has increased the significance of this attribute or value. Reid and Gilbert (2010) 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. With the loss of a hard-drive as the case of Washington State University, all this impacts the control value. 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 refers to the usefulness of information (Bey, 2012; Antirion, 2011; Wu, 2009; Parker, 2002). 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. For example, if a person encrypted an electronic record on a disk in order to prevent unauthorised access or undetected modifications, but then unfortunately lost the decryption key. This example pinpoints a breach of utility. Utility should not be confused with availability, as utility may need time to work around the change in electronic format or presentation, but usefulness is distinct from that of availability (Staffhost Europe, 2020).

Given the complexity of cyber space and the sheer size of the infrastructure, it is perhaps unsurprising that human error is an important consideration. In fact, many argue that at the level of the core backbone of the infrastructure, human error is a more significant security issue than those listed in the above paragraphs. Human error may encompass misconfiguration of devices or router or other infrastructure causing either local or, in extreme cases, regional or international issues. Mistakes and misconfigurations may go unnoticed and result in vulnerabilities that attackers can then exploit.

Having legitimate and privileged access to e-records as well as the systems has made personnel prone to defying policies and procedures and most cases become perpetrators in failing to observe security ethical values. This is because they can easily cover their tracks. For this reason, among others, vetting of personnel is vital to determine suitability of individuals for employment or transfer to a different department. According to George et al. (2019), organisations choose to perform due diligence and vetting of candidates when they are hired, promoted, or redeployed. These checks reveal information about a job candidate's character, reputation, and experience by reviewing data such as financial information, civil records, education, licensing, criminal records, and employment history.

The literature reviewed has provided useful insights and the foundation for this paper. However, it seems to fall short in putting emphasis on the principles of security ethical values considering the ever-evolving digital space and the security issues that come along in the management of records within a university setting. Further, the literature has not covered security ethical values as an area with multidimensional complexities that invites intelligence of professionals in different fields from information sciences, computer sciences and human resource, to mention but a few, and the stakeholders that include top management, deans, directors, heads of departments, records managers, actions officers among others. This paper brings out fundamental principles that will contribute to the existing knowledge by guiding the attention of organisations including Moi university to shift to the importance of being solid in adopting a variety of measures and strategies of securing records. These include practising security ethical values and investing in the understanding of the cyberspace dynamics. In particular, this paper seeks to address the gap by providing a platform for processes, controls, policy and regulatory regime for security ethical values in order to enhance integrity, accountability, transparency and ethical conduct in records management. It also provides the framework for staff training and infrastructure development.

3 Methodology

This paper is part of a doctoral thesis that was conducted using a pragmatic paradigm and an embedded case study research design. The target population of 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 at Moi

University, Kenya. A complete enumeration of the population was taken. Therefore, a choice of sample size was not necessary. The target number of respondents for interviews was 23. However, those reached for the interviews were 21. In particular, 5 response rate was achieved from top management as well as 16 from deans of schools and directors of directorates. From questionnaires out of 122 sent out, 118 were duly completed and returned. The questionnaires were administered to action officers, records managers and records staff, while interviews were conducted with top management, deans of schools and directors of Information Communication Technology as well as Quality Assurance directorates. Qualitative data were analysed thematically and presented in a narrative description while quantitative data was organised using Statistical Package for Social Sciences (SPSS version 24) and summarised by use of descriptive statistics for ease of analysis and presentation by the researcher.

4 Findings of the Study

The findings of the study are presented here according to the key themes anchored on the specific objectives of the study.

4.1 Understanding if e-records security ethical values were achieved at the University

The paper sought to find out whether the security ethical values of confidentiality, integrity, availability, authenticity, control, and utility of e-records are achieved in Moi University. The results from interviews showed that 12 (57.1%) of the respondents held the view that e-records security ethical values were achieved, 7 (33.3%) indicated that some of the ethical values were not achieved, and 2 (9.5%), in contrast, indicated they were not achieved entirely. However, it is difficult to attain 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 and R9:

According to R7:

> *These (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. However, with the decentralised nature of running of the university affairs especially in schools and departments each department takes control. In our case, we sensitise users on how to handle confidential, internal information among others. On issues of integrity, we store e-records on servers, and there is limited access to those records. On 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 authenticity is lost then 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 the 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, IPads, mobile phones and external storage devises to thieves, both on campus and outside campus, has led to the loss of vital e-records and other information. Most of the devices are not encrypted and lack passwords. This has led to compromising the 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 1.

Table 1: 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 2.

4.2 Vetting of staff in meeting the ethical values

The respondents were asked whether vetting of staff is carried out. 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.*

Table 2: E-records security ethical values (n=118)

		Responses		
		N	Percent	Percent of Cases
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 Discussions of results

The findings 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 school or department affairs, lack of guiding principles and weak implementation of classification of e-records, the security of the information is at 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 that protected financial records of the university. From the questionnaire, the findings revealed that 19.7% of the respondents agreed that availability of e-records was achieved, and another 15.9% 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 was 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. These records should not be made available or disclosed to unauthorised individuals, entities, or processes/systems. 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 personnel only. This is because a breach of confidentiality may be prejudicial to the interests of the organisation and/or its users (Northeastern University 2018; Bristol clinical commissioning group, 2016; Steichen 2012; Mishra 2011).

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 stop 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 programmes is also a setback to the university's existence. In the digital environment, if records are not managed professionally, the integrity and value such as legal evidence and as an authoritative source of evidence for the university may easily be compromised (Wamukoya, 2013). This implies that Moi University should be vigilant in the digital space to protect e-records from the unseen cybercriminal attacks with the help of the fast-developing trends in cybersecurity.

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 finance, accommodation, and examination that are integrated making the access of e-records by concerned stakeholders easy and without a hitch. Availability is the 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 that 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 that contain them as well as providing the same to users (Qadir & Quadri, 2016; Frank, 2016; Gladden, 2015; Bey, 2012; Antirion, 2011).

The university preserves authenticity in many ways. According to the findings these include referring to the authors at a given level to allow access as well as use of physical and administrative controls. The literature asserts that an authentic e-record is one that can be proven to be what it purports to be; has been created or sent by the person purported to have created or sent it; and has 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 from (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 that they were not 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 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 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).

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 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 should not be the case (Staffhost Europe, 2020). 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 values 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).

6 Conclusion

The findings indicated that ethical values of confidentiality, integrity, availability, authenticity, possession/control and utility were practised to some extent in the university. However, with the decentralised nature of running the university affairs, especially in schools and departments, and the lack of guiding principles, the security of the e-records 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 rigour in terms of protecting financial records compared to human resource records and student records which easily leaked and were shared superfluously.

Moi university has many reasons for taking a proactive and repetitive approach in tackling matters to do with security ethical values. Dedicating supreme attention and giving priority to e-records security issues can determine how best to effectively approach security ethical values in the current digital democracy era. Thus, best practice mechanisms may sustain the institution. This implies protecting valuable e-records as well as the systems ensuring that at all times only authorised individuals or systems and software have access. Hence, the process of controlling access be based on a pre-established role-based privilege having in mind the complexity brought about by the nomadic computing that brings about attacks from external sources which include hackers and viruses just to mention a few.

7 Recommendations

From the foregoing, the study recommends as follows:

1. Records management practitioners in the university need to work hand in hand with other departments to ensure that they fully understand the technological infrastructure that supports e-records management. These may include senior members of management, human resource management, the department of ICT, financial department, division of administration, planning and development. By working together, all these departments will bring a common understanding since all of them have unique roles and cover the major business processes and functions of the university. This group, led by a senior member of management may discuss, develop and implement matters regarding university business process and the records generated, systems and network architecture and infrastructure, and security requirement, among others.

2. In liaison with the ICT department, the records personnel should consider developing a robust set of ideas and principles to underpin new approaches in e-records management with application of security values bearing in mind the continuous development in technology.

3. The rapidly changing technological environment calls for Moi university to adhere to best practices, governance and compliance pertaining to security control requirements in electronic records management. This may entail placing greater emphasis on proper creation, capture and management of e-records, the systems that hold them, their business context and identifying requirements for their management over time. This calls for the records management and ICT departments working hand in hand with the support of top management in developing relevant policies. These may include records management policy, security policy, and human resource policy, among others, that provide guidelines on major business processes and the requirements to be adhered to.

4. The university should also consider adopting a security management standard ISO/IEC 27001:2014 and also records management standards including ISO 15489:2016, KS 2229:2010 on e-records management systems - functional requirements; KS ISO/TS 21547:2014 on health informatics - security requirements for archiving electronic health records guidelines; KS2374:2012 e-records management systems implementation guide; KS2391:2013 on electronic signatures - metadata requirements, that should be customised to fit the business needs of Moi University.

5. The Human resource department should ensure that personnel or those to be recruited have gone through a given kind of vetting process to determine suitability of a candidate, especially in a department with sensitive e-records and information. The receiving (of a personnel) department should also take into account the potential impacts of a personnel not vetted, this should be well stipulated in the recruitment policy. Vetting should be carried out periodically and continuously to minimise on insider threat, neglected actions and other negative events that may impact negatively the image of the university.

6. The personnel not only pose greater threat to an organisation but are also the most vulnerable link to cyber criminals. The records management department should prepare a detailed budget giving justification on why the university should invest in the management of e-records activities. The department should make a presentation to the top management justifying the rationale behind having continuous awareness and trainings on cyberspace and cybersecurity threats to technological infrastructure and e-records and the importance of embracing

proper strategies in enhancing security ethical values in management of e-records. Involving the top management may also assure support and goodwill for the implementation of the trainings and awareness programme.

References

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

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

Australian National University, (2019). ANU releases detailed account of data breach[online] https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach (accessed 15 July 2020).

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

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).

Bristol Clinical Commissioning Group. (2019-2021). Records management policy. [online] https://bnssgccg media.ams3.cdn.digitaloceanspaces.com/attachments/BNSSG_CCG_Records_Management_Policy_Sep_19_v1.pdf (accessed 10 may 2020).

Chapple, M. (2019). Security, privacy and confidentiality: What is the difference[online] https://edtechmagazine.com/higher/article/2019/10/security-privacy-and-confidentiality-whats-difference (27 August 2020).

Clemmer, L. (2010). Information Security Concepts: Authenticity [online], Available http://www.brighthub.com/computing/smb-security/articles/31234.aspx, Accessed 11, 2018.

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

DOD 5015.02. (2007). Electronic records management software applications design criteria standard. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/501502std.pdf (accessed 21st August 2020)

Frank, 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.

George, A., Arey, B., & Ertzinger, B. (2019), Best practices in vetting prospective and current employees. (online) https://www.dhs.gov/sites/default/files/publications/ia/ia_best-practices-vetting-prospective-current-employees-v2.pdf. (accessed 1st August 2020).

Groch, S. (2019). ANU data breach: How hackers got inside Australia's top university. [online] https://www.canberratimes.com.au/story/6414841/like-a-diamond-heist-how-hackers-got-into-australias-top-uni/ (Accessed 15th July 2020).

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).

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 Records Management Trust. (2016). Digital Preservation in Lower Resource Environments: A Core Curriculum: Managing Metadata to Protect the Integrity of Records. London. IRMT.

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

Ismail, A. & Jamaludin, A. (2009), Towards establishing a framework for managing trusted records in the electronic environment. *Records Management Journal*, 19(2), 135-146.

*ISO 15*489-1, (2001). *Information and documentation –Records Management-Part 1: General*. Geneva: International Organization for Standardization.

*ISO 15*489-2, (2001). *Information and documentation –Records Management-Part 2: Guidelines*. Geneva: International Organization for Standardization.

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

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

Kumar, A. & Malhotra S. (2015). Network Security Threats and Protection Models. Network Security Technical Report–CSE-10150. [online] https://arxiv.org/ftp/arxiv/papers/1511/1511.00568.pdf (accessed 14 June 2020).

Martin, A. & Khazanchi, D. (2006). Information availability and security policy. Proceedings of the twelfth Americas conference on information systems, Acapulco, Mexico August 04th-06th, 1257-1268.

Mishra, A.K. (2011). *Information security and Cyber Laws*. New Delhi: S.K. & Sons Publishers.

Moi University, (2011). *Information Communication Technology policy*. Eldoret: Moi University Press.

Musembe, C.N. & Mutula, S. (2019). E-records security classification and access controls at Moi University. In Ocholla D.N. and Neil D. E. (Eds). Proceedings of the 20th Annual IS Conference 18th-20th September 2019 on Data information and knowledge for development in Africa. South Africa, University of Zululand, Department of information studies. Rossyln Publishers, Pretoria, South Africa. (pp 138-164).

Musembe, C.N. (2019). E-records security management at Moi University, Eldoret, Kenya, Ph.D. Thesis, South Africa, University of KwaZulu-Natal.

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.

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).

Ozair, F.F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. Perspect Clin Res. 2015 Apr-Jun; 6(2): 73–76. (online) https://pubmed.ncbi.nlm.nih.gov/?term=Ozair%20FF%5BAuthor%5D&cauthor=true&cauthor_uid=25878950. (accessed 1 July 2020).

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. (2010). Our excessively simplistic information security model and how to fix it. *ISSA journal,* 12-21.

Pulseway, (2019). University data breaches in 2019 that are hard to ignore. [online] https://www.pulseway.com/blog/university-data-breaches-in-2019-that-are-hard-to-ignore (accessed 1 July 2020).

Raaen, N. (2017). *Electronic records management guide for the Judiciary*. National Association for court management records in the electronic environment. *Records Management Journal*, 19(2), 135-146. https://doi.org/10.1108/09565690910972084.

Reid, C.R. & 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.

Staffhost Europe, (2020). Cybersecurity and Parkerian Hexad (online) https://www.staffhosteurope.com/blog/2019/03/cybersecurity-and-the-parkerian-hexad (Accessed 15 August 2020).

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).

The White House, (2011). Presidential Memorandum - Managing Government Records. [online]https://obamawhitehouse.archives.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records (accessed 12 march 2020).

United Nations Programme on HIV/AIDS (UNAIDS). (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).

Unites States of America Department of Homeland Security. (2009). Understanding Denial-of-Service Attacks Security Tip (ST04-015) [online] https://us-cert.cisa.gov/ncas/tips/ST04-015 (accessed 1 August 2020).

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 2020).

Washington Post. (2019). Hackers breach admissions files at three private colleges [online] https://www.washingtonpost.com/education/2019/03/08/hackers-breach-admissions-files-three-private-colleges/(accessed 2 February 2020).

Wu, X. (2009). Security architecture for sensitive information system. Ph.D. Thesis. Australia. Monash University.