E-records security classification and access controls in Moi University, Kenya

Carolyne Nyaboke Musembe[1]

University of KwaZulu-Natal

carolyne.nyaboke@gmail.com

and

Stephen Mutula[2]

University of KwaZulu-Natal

mutulas@ukzn.ac.za

Abstract

Moi University has installed a range of computerised systems that generate a variety of e-records which when securely managed can promote accountability and good governance for enhanced service delivery. However, e-records security management at Moi University seems not to be fully compliant with international best practices through the entire lifecycle from generation to disposal. This paper (which is part of a thesis on e-records security management) therefore investigated e-records security management at Moi University with a view to offering practical and policy interventions to address this challenge,to identify how business activities are aligned to access classification, to assess how security classification of the e-records process is handled to improve access control and to establish the existence of security classification and access policies at Moi University. Data was collected from Moi University staff using interviews and questionnaires and was analysed thematically, and using the Statistical Package for Social Sciences (SPSS) version 24. Findings revealed that even though the analysis of business functions and processes was being carried out at Moi University, the University had failed to appreciate e-records classification security best practices among them; developing a classification scheme

1. Carolyne N. Musembe is a PhD student at the University of KwaZulu-Natal, South Africa and a lecturer at Moi University, Kenya

2. Stephen Mutula PhD is a professor, Acting Dean and Head of School: MITG, University of KwaZulu-Natal.

and a policy guide on security classification. The study further established that although the university had access controls that depended on user role privileges and the principle of least privilege, unauthorised access to classified e-records and systems by personnel with requisite privileges and stolen access credentials belonging to fellow personnel members was prevalent. The study recommends that the university should develop and enforce e-records management policies that integrate matters of security

Keywords: E-records; e-records management; security classification; access controls

Introduction and background

Adoption and implementation of information systems in organisations worldwide have become indispensable as a result of the on-going rapid technological advancements. As early as the 1990s, there existed information and records management systems. (Marutha 2019; Katuu 2012). The primary purpose of this information system is to facilitate business transactions and process so as to generate, receive, manage, disseminate and administer and provide access to the e-records and other information needs, including artificial intelligence between an organisational unit and its clients.

Embracing technology is an indication of acceptance by organisations that e-records can be admissible in a court of law, be compliant with regulatory and statutory requirements, meet audit requirements, be used for decision making and other purposes depending on the ability to establish their authenticity, reliability, integrity, availability, control, and utility by indicating the dependability of the systems used to generate them. Thus, e-records management has become an integral tool of governance that enables institutions to create and maintain dependable evidence of business processes in the form of electronic records. This is possible when e-records provenance can be traced and the information is complete and accurate in content, context and structure and can be located, retrieved, presented and interpreted (Kenya Electronic records and data management standard, 2016).

E-records security management also entails the developing, implementing, monitoring, reviewing and providing of a necessary improvement on e-records security policies, procedures, processes, organisational structure, and information system functions. These coordinated activities enable protection of e-records and the information systems through defining, achieving, maintaining and improving their security effectively and efficiently, which is essential to the organisation's achievement of its core business processes and maintaining its legal compliance, business continuity, competitive edge, growth and image and quality service delivery among others (ISO, 2014; ISO, 2012; Parker, 2002).

Personnel play an essential role in the implementation of e-records security management. Therefore, organisations have the responsibility of ensuring that they have a support system in terms of human resources (personnel) who are competent and reliable to enhance e-records security. Many authors, however, have indicated that personnel are the major threat to e-records security management practices in organisations. They habitually do not see themselves as part of the organisations e-records security 'effort' and often take actions that ignore organisational e-records security best interests. These actions may include but are not limited to knowingly or unknowingly damaging information systems and stealing information for personnel, destroying or deleting critical e-records of the organisation or personnel and unauthorised sharing of access privileges, thus providing access to vital information of the organisations' operations by unauthorised individuals among others (National Association County & City Health Officials (NACCHO), 2015; Andersson, Reimers and Barreto, 2014; Bey, 2012; Parker, 2002). Altogether, personnel of an organisation can easily espouse an organisational culture which can impact positively or negatively on the organisation's e-records security management culture. A study by Tucker and Pitt (2009) on customer performance measurement in facilities management established that organisations' culture is the combination of shared values, behaviour patterns, moves, symbols, attitudes and normative ways of conducting business. This implies that with the right culture, awareness and continuous education, personnel can highly support organisations' efforts towards achieving e-records security management practices. Consequently, Roer and Petric

(2017) ascertain seven critical dimensions of e-records security culture in organisations that should be natured in personnel: right attitudes, behaviour, cognition, communication, compliance, norms and responsibilities.

E-records security management is a broad area and this paper will dwell on e-records security classification and access control as part of the process and practices of e-records security management. E-records classification is a well-established practice that originated from the military (Bergstrom, 2017); however, it has not been given the utmost attention in many organisations despite enabling determination of the value and level of sensitivity of various information held by an organisation. In addition, classification and access control provide a better understanding of e-records and how and why they need to be protected. That is; they reduce threats of information leakage, help in the identification of e-records suitable for routine dissemination or for disclosure in the event of a request, protection of the rights and interests of the organisation, its staff and its stakeholders; it enhances compliance with legal and statutory requirements, and demonstrates organisations' commitment to good governance. Despite e-records security classification being vital, most organisations face difficulties in its development and implementation. In addition, there is little literature on e-records security classification to enhance its implementation. For instance, the existing methods described in standard works do not provide a coherent and systematic approach to e-records classification. Niemimaa and Niemimaa (2017) assert that the implementation of information classification standards describes the practice of information classification in a general and universal manner without explaining how the practice could be applied in any particular organisation. Further, there is a lack of detailed descriptions regarding the synopsis of the processes, procedures and concepts, roles involved in the classification and how they interact, how to modify the method for different situations and a framework that structures and guides the classification.

Problem and purpose of the study

Moi University has a range of computerised systems such as Integrated Personnel and Payroll Data System (IPPDS), Financial Management System (FMS), Hostel

Booking System (HBS), Examination Management System (EMS) among others that generate a variety of e-records. The e-records generated must be securely managed to promote accountability and good governance for enhanced service delivery. However, e-records classification management and access control at Moi University is not fully compliant with international best practice through the entire lifecycle from generation to disposal. This paper, therefore, sought to investigate e-records security classification and access controls at Moi University with a view to offering practical and policy interventions to address this challenge. To investigates e-records security classification and access controls at Moi University with a view to offering practical and policy interventions to address this challenge,. the study addresses the following three research tasks:

- To identify how business activities are aligned to access classification.
- To assess how the security classification of the e-records process is handled to improve access control.
- To establish the existence of security classification and access policies at Moi University.

Theoretical framework and literature review

The main aim of this paper was to investigate e-records security classification and access control at Moi University. As indicated in the abstract, this paper is part of a thesis on e-records security management at Moi University, Kenya. The study was underpinned by Records Continuum and Parkerian Hexad models. The Records Continuum model is vital to this paper since its emphasis is continuous management of records, from the moment records are created (and even before creation) and maintained until they are disposed of. It also focuses on providing sustainable record-keeping to connect the past to the present and the present to the future. Moreover, the Records Continuum Model recognises e-records from creation to disposal as part and parcel of the business process of an organisation.

This paper examines, among others, how the security classification of the e-records process is handled to improve access control. Thus the model ensures the creation of the right e-records containing the right information, in the right formats; the 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 to enhance access (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 Records Continuum Model is most suitable to help manage such records in order to improve responsiveness, increase efficiency and satisfy user requirements. For these reasons, Moi University should provide an environment that supports e-record-keeping and security measures to enable proper creation and maintenance.

Even though the 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 place much 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. For these reasons, the Parkerian Hexad (PH) model was applied to enhance the study.

The PH model is relevant to the study since it strongly advocates 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 in it a more daunting task. The PH model encourages organisations to invest in better policy writing and enforcement procedures and methods, employee education and awareness, and improving the available technology infrastructure, as one of the objectives of the paper is to identify the existence of security classification and access policies at Moi University

Moreover, the elements of the PH Model (which include confidentiality, integrity, availability, authenticity, possession/control and utility) 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 over time and ensure efficient access. One of the objectives of the study is to identify how business activities are aligned to access the classification of e-records at Moi University. Therefore, the model is vital to understanding the University's position on the e-records security classification and access to e-records. As 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. The following is a brief literature review.

Security classification of e-records

Organisations generate, receive and manage a massive variety of e-records that must be protected from unauthorised access, disclosure, misrepresentation, modification, and other security threats. This is made possible by applying the right process and procedures and having in place proper systems and systemic requirements. Classification enables an organisation to understand its e-records' sensitivity, value, criticality, nature and impact of an unauthorised disclosure in relation to legal and regulatory requirements among others (Plymouth University, 2017; The University of Newcastle, 2017; City University of Hong Kong, 2015). It instigates with 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 organisations 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 the 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.

To understand e-record classification, an analysis of the business process should be carried out. This 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 (2009) asserts that far too many good records management programmes are suffering from a 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 is the organisation's strategic assets, analysing the processes yields 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 (Tasmania Archive Heritage Office (TAHO) ,2015; ICA, 2008; DIRKS manual, 2003; 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 all ICT systems and the e-records therein regardless of technology used, 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). It is essential for the organisation or university to guarantee that the classification process is understood to be a ‘living process’, that is, e-records security

classification is not a one-time process and procedure but carried out regularly and periodically reassessed to enhance requisite security (TAHO, 2015). Further, 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 a means to secure them. This gives the measure by which an organisation assigns a level of sensitivity and ownership to each piece of e-records that it creates, receives and maintains (Public Service of Kenya, 2010; Mishra, 2011).

Various factors influence the e-record security classification. Mishra (2011) in a study of information security and cyber laws in New Delhi, India, outlined considerations in the 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 and the nature of the organisation are also important considerations when classifying e-records.

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, the National Archives of Australia prepared an overview guide on classification tools that could assist Commonwealth countries to support records management processes. Furthermore, the State Records Authority of New South Wales and the National Archives of Australia ISO have developed guidelines that can be applied globally in e-records security classification, among others. Therefore, organisations should adopt an e-records security classification process to be able to apply the right level of classification. This may include but is not limited to analysis of a business process (understanding the process activities, functions of the organisation), identify the e-records and the information systems available (multiple media types and formats of e-records), identify the creators (the organisation should ensure that there is a

custodian that is authorised for the classification and is responsible for establishing, implementing and maintain the e-record), undertake impact assessments (once an e-record is classified, the date and the event can be easily determined, after which the consequences of compromise might change.

However, an event may trigger an increase in the sensitivity of the e-record; for instance, a personnel dependants form may be public when not filled in, after which it is confidential. Other issues may include e-records control, encryption, blending of the e-records with other organisation e-records; if a security breach does occur, is damaged or destroyed, e-records backup frequencies. Conventions or standards and availability of an audit trail to demonstrate the university data are reliable), apply classification-based controls (appropriate controls must be applied to ensure the protection is given to the e-record commensurate with the security classification. For instance, a need-to-know principle, clear desk policy to stop unauthorised personnel from using any classified system or e-record; classified e-records from external sources should retain security classification as forwarded), document and maintain e-records security classification register (the organisation should be able to be reviewed, updated and maintained periodically, and an e-records security classification register indicating all e-records classified and the level of classification), audit logs (to enhance and maintain integrity, authenticity, utility, availability and confidentiality of the e-records a strict logging process is to form part of the e-records classification register. The audit log must be well designed to enhance its capability of capturing a ‘trail of evidence’ which can be used to investigate inappropriate, unauthorised or illegal access) education and awareness (this should be a continuous process from the induction of the personnel to enable them to understand the prominence of security classification to e-records and information systems and other computer technologies (Griffith University, 2019; University of Southern Queensland,2018; TAHO, 2015)

ISO (2013), however, asserts that an organisation should avoid using too many classification categories, as complex schemes may become harder and uneconomic to use. Thus, e-records security classification may be ascribed as restricted (this

classification label is applied to e-records, information systems and computer technologies that are very sensitive in nature and are strictly confidential to the university, the government or any other legal agreements between the university and third-parties, for instance, consultants or service providers, contractors, researchers as required by the scope of the activity at hand). The e-records are considered critical to the university's capacity to conduct its business process. Their disclosure could cause severe harm to the university's reputation, its personnel, students and third parties. They are accessible to relevant personnel with specific roles or positions and business partners with appropriate authorisation. Examples of the e-records may include examination papers before being released, personnel data, privileged accounts' passwords of the university's key information systems, pending criminal investigations, social security numbers, financial account numbers, medical records among others) (Griffith University, 2019; University of Plymouth, 2017; City University of Hong Kong, 2015; Kahanwal and Singh, 2013 Mishra, 2011; Collette and Gentile, 2006; DoD, 2002).

Secondly, *confidential* (this classification is applied to sensitive information that is intended for use by a specific group of authorised personnel within the university and business partners assigned on a need-to-use basis and for an authorised envisioned purpose. It is accessible to only specified and authorised personnel with prerequisite credentials. A breach could cause unacceptable damage to adverse and lasting consequences threatening the university and its activities. Examples here include student information, personnel financial information, patent(s) pending, students' and staff disciplinary details, unpublished research information and identifiable research subject information) (University of Exeter, 2018; University of Plymouth,2017; City University of Hong Kong, 2015; Mishra, 2011; DoD, 2007 Collette and Gentile, 2006).

Thirdly, *internal use*; the classification is assigned to non-sensitive operation e-records. The information contained therein is intended for use within the university or organisation (authenticated personnel) and authorised service providers. A breach of such e-records may have moderate to adverse implication and access may be provided free to a specific group of personnel depending on their roles and

responsibility. They include policies, unpublished research, a notice of meetings, seminars, training materials, advertisement, manuals, and procedures) (University of Exeter, 2018; University of Plymouth, 2017; City University of Hong Kong,2015; Kahanwal and Singh, 2013).

Fourthly, *public* (the information in this category, can be used by both personnel and members of the public without restriction, although it should not be placed in the public domain without a proper reason. That is, approval by authorised parties should be considered before being released for public consumption, having in mind the information's utility, accuracy and completeness prior to release. The information may include academic programmes and admission information, press releases, published academic literature (Griffith University, 2019; University of Exeter, 2018; University of Plymouth,2017; City University of Hong Kong, 2015; TAHO, 2015; Mishra ,2011; DoD, 2007; Collette and Gentile, 2006;)

Fifthly, *private* (this classification is a default classification in most organisations and universities referring to their information assets. Access may be open to all personnel and external authenticated third-parties) (Griffith University, 2019). Sixth is protected, (somewhat, very little information belongs in this category thus it is used with restraint. Thus, this classification requires a substantial degree of protection, as disclosure may cause serious harm to the organisation or university, personnel or students. The e-records that fall in this category may include highly sensitive communication between the university and the government, executive management or council matters of a highly sensitive nature, litigious or law enforcement information, the loss and/or compromise of which would seriously jeopardise the university, significant inquiries or investigations that are likely to cause serious harm to individuals, groups or the general community, for instance crime and corruption enquiries, highly sensitive financial and economic information) (Griffith University, 2019; TAHO, 2015).

Although e-records classification is important, maintaining a security classification beyond its utility is costly and administratively burdensome, thus organisations should ensure they establish at the time of classification the period the e-record remains

classified (Executive office of the president of the United States classification guide, 2018). This is consistent with TOHA (2015) sentiments that e-records, information systems, and computer technologies must be declassified or downgraded when protection is no longer required or is no longer required at the original level. If a user believes that an e-record, for example, has been incorrectly security classified, they must advise the custodian or owner who may consider the need to reclassify the e-record. Ideally, the e-records declassification triggers will be set when the initial classification is applied and should be captured in the e-records classification register. Perhaps the declassification triggers may include a set time period after the creation of an e-record or system, passing of a set date for review, after circumstances that have a direct impact on the e-record or information system change significantly, such as a change of strategic priorities or a change of government, among others.

Nonetheless, the classification category varies from one organisation to the other. The Public Service of Kenya (2010) asserts that the 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).

E-records access control

During security classification, the person should consider access control since the classification alone will not stop unauthorised personnel from accessing the e-records in any way unless proper access controls are adopted. The computer technologies embraced by organisations should enable access to e-records from autonomous end-points to enhance efficiency. The e-records should also be available in real-time to enhance real-time decisions and actions to authorised personnel and third parties.

Protecting information systems, applications and e-records against unauthorised access are vital in e-records security. This denotes that e-records management systems should guarantee complete, organised, accessible and secure records which are compliant with legislative, regulative and appropriate business requirements, reflecting a comprehensive range of appropriate business activities and systematic creation. For these reasons, the acceptance of e-records for legal compliance, audit decision making, and other purposes is contingent on establishing the authenticity, integrity, utility, reliability of the systems used to generate them (Kenya electronic records management standard, 2016)

To enhance access control organisations should grant limited access on a need-to-have basis, use of strong access credentials (including passwords, PIN, passcode, biometrics), use a multi-factor authentication, hardening computer systems, deployment of security technologies such as firewalls, antiviruses, intrusion detection systems among others, use of encryption where applicable, regular software updates, maintain and monitor logs, conduct systems vulnerability assessments, penetration testing and remediate and conduct user awareness (Communication Authority of Kenya, 2018; TAHO, 2015). Further, a formal access control matrix (user registration process to enable assignment of access rights) must be developed to record role-based authorised access on an individual basis (Uasin-Gishu county ICT policy, 2016). This may include the provision of unique user identification (ID) or credentials to enable users to be linked to and held accountable for their actions; the use of shared ID's should only be permitted where necessary for business or operational reasons and should be approved and documented. Immediate disabling or removal of IDs of users who have left the organisation should also be observed as part of access control. (Kenya information security standard,2016).

Role-based access control is a method applied successfully by many organisations to link access rights with the business process to enhance e-records security. 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. 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). 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 the 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 enable the efficient retrieval of information. They further stated that confidentiality and accessibility should concurrently be adhered to through proper classification, labelling, indexing, and file naming.

ISO (2001) reiterates that an 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 classification to establish whether the activity and the business area are identified as areas of risk or have security considerations and/or are legally required restrictions and to establish the appropriate control mechanisms for handling and recording the access or security status of the record in the system to signal any need for additional control measures. Hence, assigning rights and permissions to user accounts associated with a role among others must be done appropriately and be consultative 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 records. (TAHO 2015. ISO (2001) advise 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 and 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.

Security classification and access policies

Accordingly, organisations have to consider establishing and implementing an access control policy based on the business process and e-records security requirements. The policy should take into account the security requirements of business process, policies on information dissemination and authorisation, for instance, a need-to-know principle, e-records security levels, and e-records classification, consistency between the access rights and e-records classification policies of systems and networks, roles with privileged access, removal of access rights, archiving of records of all significant events concerning the use and management of user identities and secret authentication information and management of access rights in a distributed and networked environment (Kenya information security standard, 2016; ISO/IEC, 2014; ISO, 2001).

Kenya's 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 so as to promote accountability, transparency and public participation and access to information. Under the Act, entities 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.

Research method

The paper 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 classification and access control 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 target population for quantitative data 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 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. Only qualitative data by interviews are reported in the next section.

Findings

The findings are reported in Sections 1.1 -1.3. Only qualitative data by interview are reported in the findings for this paper

1.1 Aligning business activities to access classification

To understand security classification, the respondents were asked about the roles they played in business activity analysis of the University. All the 16 respondents (deans and directors) noted that they are involved in the business activity analysis. For instance, 14(87.5%) reported that they are involved in business activity analysis at school level, university senate level and dean's committee level in the areas of academics, financial, planning and administration, student affairs, staff matters, outreach, research, community services among others. Another 2 (12.5%) (directors) were also involved in business activity analysis like their counterparts to fulfil the requirements of their directorates, that of quality control on the 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 academics, 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, a 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 were further asked how business activities are aligned to enhance 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.*

The 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 that there is some security classification that is applied. Though a majority,19 (90.4%), of the respondents indicated that there was no clear guideline and direction, 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 a minimal number of users including e-records from deliberation of the University Council, fiscal records, student examinations among others; 'public' those accessed by both members of staff and the community, including notice of upcoming events that is sports, requests for tenders, medical campaigns, 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.

1.2 How the security classification of the e-records process is handled to improve access control

The respondents were also asked on how the 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 the university council are not accessed by anyone, but those with the 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 of.

The responses are summarised in the 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 superuser 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 secure 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 they were 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.

1.3 Existence of security classification and access policies

On whether they were aware of the security classification and access policies 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 assigns them 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 item 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 the 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 determine whether the university has a user permission register and how it distinguishes the privileges of the user. However, all five 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.

Discussion

E-records are a product and a strategic asset that reflects the business process of a university. 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 were minimal and decentralised. Each department or school has its way of managing security, since there are no guidelines and programmes 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 are thought of as an ICT function, which should not be the case. Despite the ICT directorate playing a major role in the ICT infrastructure, they may not fully understand 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 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, processes or procedures and activities that lead to the creation of e-records of the University are understood and practised.

The literature reviewed indicated that to improve business processes, the same should be analysed in order to understand the activities, their relationship, and values of their relevant metrics. The literature further indicated that an analysis of a business function of an organisation is vital for it links the business process to e-records. It further indicated that business analysis is a clear way of developing a 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 (Glavan and Vesna, 2017; ISO, 2001; AIIM ,2009). Similarly, the continuum model observes that business activities are created as part of the business communication process within and without the organisation and advocates intellectual control of e-records management actions. The e-records management actions include classification of records within a logical system (Upward, 2004; Xiaomi, 2003). From the study findings, it is evident that 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/or 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 include 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 is based on the nature of the information and the level at which the e-record was generated. This includes ‘top secret’ (including deliberations of the

University Council, student 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 reviewed provides similar but more secure classification techniques depending on the nature of the organisation (Griffith University, 2019; University of Plymouth, 2017; City University of Hong Kong, 2015; Kahanwal and Singh, 2013 Mishra, 2011; Public Service of Kenya, 2010; DoD, 2007). 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, prevent illegal entry, enhancement of staff safety, reduction of security cost and facilities management, among others. ISO (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 processes, 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 by 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.

Conclusions and recommendation

The university has not fully appreciated e-records security classification and access controls including developing a classification scheme and a written instruction on security classification to provide sensitive e-records that legally require restrictions and the duration of the restriction. Although the university had in place access controls that depended on user role privileges and the principle of least privilege, 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 fellow personnel. These findings identified personnel as a significant threat to information security. The study recommends that 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 an 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.

References

Andersson, D., Reimers, K. and Barreto, C. (2014). Post-secondary education network security: results of addressing the end-user challenge. Proceedings of INTED2014. Conference 10th-12th March 2014, Valencia, Spain.Retrieved from *https://library.iated.org/view/ANDERSSON2014POS* (accessed 2 March 2019).

Association of Information and Image Management (AIIM) .(2009). Electronic records management –still playing catch up with paper. Retrevied from *https:// www.aiim.org* (Accessed 18 August 2017).

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, 371-382.

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

Bergstrom, E. (2017). A method for information classification, (thesis proposal), University of Skovde. Retreived from: *http://his.diva-portal.org/smash/get/ diva2:1162686/FULLTEXT01.pdf*

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

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.

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

Centre for Development of Security Excellence (2017). 2017 year report. Retrieved from *https://www.cdse.edu/documents/cdse/2017-year-end-report.pdf* (accessed 1 October 2018).

City University of Hong Kong (2015). Information classification and handling standard. Retrieved from *https://www.cityu.edu.hk/infosec/isps/docs/pdf/04.CityU%20-%20Information%20Classification%20and%20Handling%20Standard.1.1.pdf.*

Charles Darwin University (2017). Records disposal schedules: higher education teaching and learning of the University of the Charles Darwin University.Retrieved from: *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).

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

DIRKS manual (2003). Manual for the design and implementation of recordkeeping. Retrieved from *https://www.google.com/search?client=firefox-b-d&q=Manual+for+the+Design+and+Implementation+of+Recordkeeping+Systems* (accessed 9 June 2017)

Executive office of the president of the United States classification guide (2018). Retrieved from *https://ustr.gov/sites/default/files/foia/ Classification%20Guidance. pdf*

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.

Griffith University(2019). Information security classification framework. Retrieved from *https://policies.griffith.edu.au/pdf/*

Information%20Security%20Classification%20Framework.pdf (accessed 9 June 2019).

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

ISO 15489-2, (2001.) *Information and documentation – Records Management-Part 2: Guidelines*. Geneva, International Organization for Standardization. *Information technology-security techniques-information security management systems overview and vocabulary.* Geneva, International Organization for Standardization ISO.

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

Kahanwal, B. and Singh, P.T.(2013). Towards the framework of information security. Retrieved from *https://arxiv.org/pdf/1312.1460.* (accessed 7 May 2018).

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

Kenya Electronic records and data management standard 2016. Government ICT standards Retrieved from *http://icta.go.ke/pdf/ Electronic%20Records%20Management%20Standard.pdf* (10 June 2019).

Kenya government ICT standards. (2016). Information security standard. Retrieved from *http://icta.go.ke/pdf/Information%20Security%20Standard.pdf* (10 June 2019).

Marutha, S. N., and Ngulube P.(2018). Enterprise content management system implementation readiness to improved medical records management in Limpopo Province, South Africa, library philosophy and practice (e-journal) 1769.

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

National Archives of Malaysia (2011). Electronic records management systems-system specifications for public offices. Retrieved from *http:// www.jpm.gov.my/sites/default/files/u290/ ELECTRONIC%20RECORDS%20MANAGEMENT%20SYSTEMS%20-%20SYSTEMS%20SPECIFICATION.pdf* (accessed 17 July 2018).

National association county & city health officials (NACCHO) .(2015). Cybersecurity: Risks and recommendations for increasingly connected local health department. Retrieved from *https://www.naccho.org/uploads/downloadable-resources/Issue-brief-on-Cybersecurity-NA639PDF.pdf* (accessed 9 June 2018).

Niemimaa,E., and Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices. *European journal of information systems*, 26(1), 1-20.

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).

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.

Plymouth University (2017). Using the information security classification-guidance for staff. Retrieved from *https://www.plymouth.ac.uk/uploads/production/document/path/6/6013/EIM-GDL-001_-_Using_the_Information_Security_Classification_-_Guidance_for_staff_v1.0.pdf* (accessed 9 June 2018).

Public Service of Kenya. (2010). Records Management Procedures. Manual for the Public Service.

Roer, K. and Petric, G. (2017). Deep insights into the human factor – the security culture report. Retrieved from h*ttps://www.researchgate.net/publication/316715557_Deep_insights_into_the_human_factor_-_the_security_culture_report_2017* (accessed 9 June 2019).

Tasmania Archive and Heritage Office.(2015). Information management advice 34 implementing information security classification in EDRMS. Retrieved from *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).

The Kenya access to information act no. 31 of 2016. (2016: Retrieved from *http://kenyalaw.org/lex/actview.xql?actid=No.%2031%20of%202016* (accessed 21 October 2018).

The University of Newcastle (2017). Information security data classification procedure. Retrieved from *https://www.newcastle.edu.au/__data/assets/pdf_file/0008/348290/Information-Security-Data-Classification-Procedure.pdf* (accessed 1 June 2019).

Tucker , M. and Pitt, M. (2009). Customer performance measurement in facilities management: a strategic approach. *International journal of productivity and performance management* Vol.58 no5,407- 422.

Uasin-Gishu county ICT policy (2016). Retrieved from *https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjoq4Cc5fziAhVpzoUKHZfMANUQFjABegQIBhAC&url=https%3A%2F%2Fwww.uasingishu.go.ke%2Fdownload%2F278%2Fict-e-government%2F31187%2Fug-ict-policy-3.pdf&usg=AOvVaw3wLFf-JkbXxxtAHJBgw3W1* (accessed May 30 2019).

University of Exeter (2018). Information classification policy. Retrieved from *https://www.exeter.ac.uk/media/level1/academicserviceswebsite/it/recordsmanagementservice/policydocuments/Information_Classification_Policy_v2.pdf.* (accessed 9 June 2019)

University of Plymouth (2017). Using the information security classification-Guidance for staff. Retrieved from *https://www.plymouth.ac.uk/uploads/production/document/path/6/6013/EIM-GDL-001_-*

_Using_the_Information_Security_Classification_-_Guidance_for_staff_v1.0.pdf. (accessed 9 June 2019).

University of Southern Queensland (2018); information asset and security classification procedure. Retrieved from *https://policy.usq.edu.au/documents/13931PL* (accessed 30 May 2019).

University of Tasmania (2014). Records security guidelines.Retrieved from *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. (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 Defense (DoD) 5015.2, (2007). *Electronic records management software applications design criteria standard for electronic records management software applications*.

Xiaomi, A. (2003). An Integrated Approach to Records Management. *The information management journal*, 37(4),24-30.

Yorkland Controls Ltd. (2007). Security access control basics. Retrieved from *https://www.yorkland.net/downloads/ag_security.pdf (accessed* 15 May 2018).