


Original Research

Information Systems Security Policy Framework for enhanced ICT Governance in Public Institutions of Tanzania

Authors

Adam Semlambo 
The Open University of Tanzania
Email: semlambo@gmail.com

Edison Wazoel Lubua 
Institute of Accountancy Arusha
Email: elubua@iaa.ac.tz

Catherine Mkude 
The Open University of Tanzania
Email: catherine.mkude@out.ac.tz

Abstract

This study developed an Information Systems Security Policy Framework relevant in governing Information and Communication Technologies (ICT) in public institutions of Tanzania. It used higher learning institutions as the case for study, The framework is to guide professionals on how to secure ICT environment. Operationally, this study used a qualitative approach. It began with a review of the literature, followed by a focus group discussion to formulate new themes for the proposed Information System Security policy framework. The output of the study suggests a policy framework with the following themes: Data and information handling, Internet and network Services Governance, the use of company-owned devices, physical security, guidelines on how to acquire new hardware and software, incident handling and reporting, monitoring and compliance, and policy administration. This study recommends the use of a new comprehensive and harmonised Information Systems Security policy framework for all public higher education institutions, for a more secure environment. In addition, the study recommends additional studies including other types of organisations for comparison.

Keywords: ICT Policy, Information System Security, Policy framework, Tanzania, Higher learning institutions

1.0 INTRODUCTION

The Information Security policy provides a set of rules and regulations useful in managing the use of information resources, to maintain information confidentiality, integrity, and availability (Alinaghian, Rahman, & Ibrahim, 2011; Lundgren & Möller, 2017). The importance of the policy framework increases since institutions are more dependent on Information and Communication Technologies (ICT) than before (Kundy & Lyimo, 2019). Because of the increase in ICT uses, institutions become a target of malicious activities, from both internal and external agents. As reported by Chen and He (2013), Saunders (2017) and Herjavec Group (2017), factors such as the increase in security threats and the increase of internet users with limited security knowledge increases individual and corporate vulnerability.

This study has a special interest in public higher learning institutions in Tanzania. In the context of these institutions, the use of Information and Communication Services focuses on academic administration-associated supporting activities. These institutions use services such as student portals, online learning systems, mobile applications and associated enterprise systems (Pima, Odetayo, Iqbal, & Sedoyeka, 2016). The use of these resources is important to both learners and facilitators to equip them with reliable tools in the learning process. The increase in the use exposes these institutions to attacks; therefore, concrete measures are necessary for ensuring online safety. Traditionally, a relevant policy is one to provides proper guidance to all users on how to achieve security objectives (Mulenda & Godfrey, 2018).

According to Kahyaoglu and Caliyurt (2018), security policies are critical for information protection because they provide rules, roles and responsibilities associated with all users of the Information System. On the other hand, the study by Lubua and Pretorius (2019) suggested that the rules are the roadmap for

implementing controls, which are necessary for achieving security objectives. Because of the collective importance of security policies, international organisations (such as the International Standard Organisation - ISO) provide the baseline on generally acceptable security policies to assist all organisations in the process of securing their information systems. Standards set by these organisations are invaluable, though they are not necessarily adequate as suggested by Park (2019). This is because they don't offer a framework defining elements to be included in a security policy. Given this context, this paper developed a framework suitable for establishing Information Security policies relevant to public institutions, with a special focus on higher learning institutions in Tanzania.

2.0 LITERATURE REVIEW

This section discusses the literature related to Information Security policies and associated frameworks. First, it presents security challenges affecting higher learning institutions, followed by the theories associated with the study.

2.1 Information Security challenges affecting an organisation

Human activities require trustworthy Information Systems now than before (Almazán, Tovar, & Quintero, 2017). This is because most organisational activities are integrated to Information and Communication Technologies (ICT). For example, in Tanzania, the number of internet users increases by 4.9% per year as reported by Tanzania Communication Regulatory Authority (2022). In addition, the report by the International Telecommunication Union (2021) suggests that 50% of Tanzanians are using the internet. Users (in Tanzania and elsewhere) require online safety. Currently, users are faced with numerous security challenges as discussed in the next part).

i.) Administrative challenges

Although the government of Tanzania offers different guidelines on the safe utilisation of ICT resources, there is no dedicated Information Security policy framework that would enable institutions to develop a fresh policy document. The framework is important to offer a basic guide for every organisation while allowing them to uniquely adopt features relevant to their context. Therefore, it would provide the required administrative baselines for policy development as suggested by Hina and Dominic (2018). Apart from this baseline, the framework would guide stakeholders on procedures for policy creation and policy review (Semlambo, Leichuka & Almasi, 2022). These two elements are part of the administrative challenges facing modern organisations, including those of Tanzania. Because of this perspective, the current study developed a framework, which partly addresses the policy administrative challenges faced by modern organisations.

ii.) Technological challenges

In the context of learning institutions, technologies have revolutionised the way learning and research are carried out in higher learning institutions. Unfortunately, the use of such technologies requires adequate knowledge. Some education institutions struggle with the use of such facilities due to the lack of funds and technical expertise. As the result, they become victims of security threats (Otito, 2013). Some of the security challenges facing learning institutions and other corporations, in general,

include malware attacks, denial of service attacks and phishing (Alexei, 2021). Other risks include phishing, social engineering, supply chain assaults, zero-day and polymorphic attacks, and infrastructure attacks (Broadhurst, Skinner, Sifniotis, Matamoros-Macias, & Ipsen, 2018).

iii.) Human-related challenges

Trust is one of the human elements that affect the security of information systems (Rajaonah, 2017). Unchecked trust elements such as the exchange of login information challenge the security of organisations (Sapronov, 2020). In addition, carelessness is another human factor that affects the security of information systems (Mitra & Gilbert, 2012). Some of the careless behaviours include trusting visiting guests to use office computers, leaving workstations without logging out, introducing new software without proper training, and using outdated software and hardware. Since the organisation has employees with a mixed level of understanding, measures are important to prevent the organisation from being affected by the carelessness of its users (Patrick, Niekerk, & Fields, 2018). The current study addresses this element through a framework which will offer control elements addressing human-related challenges.

2.2. The need for Information Systems Security Policy Framework

Policy frameworks provide a set of principles that form the basis for making rules and guidelines through institutional policies (Lubua & Pretorius, 2019). This is because, a well-researched framework takes to account all threats facing the Information Society; therefore, it allows ICT policies developed to be comprehensive. Regardless of the importance of policy frameworks, not all are comprehensive. They may be affected by time factors, geographical focus or any other biased perspectives. In addition, some frameworks lack a vigour review, therefore affecting their validity. The following are some of the frameworks with their contents. The framework by Cannoy, Prashant C. Palvia and Schilhavy (2006), had the following elements: legal issues, monitoring and molarity, vulnerabilities and risks, detection, data perturbation, digital watermarking, cryptography and piracy. Balčiūnė, Ramanauskaitė and Cenys (2019) had the following elements security policies human resource security, assets management, access control, cryptography, physical and environmental security, operations security, communications security, system acquisition, development and maintenance, information security aspect of business and compliance. In addition, the framework by (National Institute of Technology and Standards (NIST), 2022) had the following elements identify, protect, detect, defend and recover, and that of Lubua and Pretorius (2019), had the following elements of data security, internet and network services governance, use of company-owned devices, physical security, incidence handling and reporting, monitoring and compliance and policy administrations.

In this case, the framework by Lubua and Pretorius (2019) is the most current. This is because it combined three other frameworks authored by Travellers Industry Company (2018), the Security Magazine (2018) and Taylor 2001, endorsed by Zednet.com. Also, it received stakeholders' input and underwent a vigour review process. Therefore, the framework by Lubua and Pretorius (2019), is used to set a basis for the future framework, that comes as a result of this study.

3.0 METHODOLOGY

The study used the qualitative approach. In the process, the study combined two key methods: document analysis and a focus group discussion. Within document analysis, the study began by setting baseline components by analysing two Information Security frameworks: Lubua Framework and the Tanzania eGovernment Security Guide framework. The resulting baseline framework is reported and used as input for the second step, which included the analysis of policies from public higher learning institutions listed in Table 1. The output of this step was subjected to a critical review of the literature to identify other elements which need to be included in the resulting framework. Finally, the study will conduct a focus group discussion to validate these results. Figure 1, presents the flow of activities.

Figure 1: Research strategy flow of activities



Source; Researchers 2022

Population and Sampling

The study focused on public higher learning institutions in Tanzania which offer Bachelor's degrees and above. Only 32 higher learning institutions qualify under this category. In this population, the study purposively and conveniently engaged 8 (eight) institutions and a total of 8 participants for interviews and 180 for focused group discussions which were obtained through saturation. Therefore, policy documents from these institutions are the ones used as cases for study. On the other hand, the study used the Lubua Framework, because it is the only available recent framework which focused on Africa but with a world view. The Tanzania e-government framework is equally used because it is a standardised framework providing basic policy guidelines for all public organisations.

Concerning the focus group discussion, one representative was purposefully identified from each represented organisation. Below are the public higher learning institutions selected as the case for the study as well as the evaluation of the new information system security policy framework.;

Table 1: Institutions selected as Case for the Study

1	Ardhi University (AU)
2	Arusha Technical College (ATC)
3	College of Business Education (CBE)
4	Eastern and Southern Africa Management Institute (ESAMI)
5	The Institute of Accountancy Arusha (IAA)
6	The Institute of Finance Management (IFM)
7	The Open University of Tanzania (OUT)
8	The University of Dare es Salaam (UDSM)

Source: Research Data (2022)

Data collection and analysis

Permission was obtained to review policies from all eight (8) public higher education institutions selected for the case study, including Lubua's cyber security policy framework. Qualitative document analysis (QDA) was used to analyse the gathered data. Similar themes were examined and grouped to find the missing gaps and inconsistencies in an adequate information system security policy framework. Morgan (2021) claims that document analysis enables the researcher to evaluate documents to give them voice and significance concerning a certain evaluation issue. It's a lot like focus group discussions or interviews because it involves putting information into groups called themes (O'Leary, 2014). Meanwhile, focused group discussion and interviews were used to conduct evaluations for each input in the new proposed framework

Quality issues

No one method can be used consistently to address the quality difficulties in qualitative research (Chowdhury, 2015). However, it may be assessed using a combination of several viewpoints, such as credibility, dependability, confirmability, ethics, and so on. The study maintained the validity and reliability of the data through consent from participants before interviews and forced group discussions were conducted. Also, the study obtained permission to use different policies from selected case institutions and Lubua's framework. Furthermore, data triangulation and crystallisation were used to attain validity and reliability.

4.0 RESULTS ND DISCUSSIONS.

This study provides the results of an analysis. The output of the study is to develop a security framework suitable for higher learning institutions in Tanzania. Figure 1 presents stages to be followed in the development process; these stages and their results are reported in the next few subsections. The following are the stages: –

- The review of existing frameworks,
- The review of existing policies,
- Literature review and
- Validation of the framework through focus group discussion.

4.1. Inputs from Information Security Policy Framework

This study selected Lubua's Cyber Security Policy Framework as the starting point for creating a new information security policy framework for public institutions in Tanzania, with a special focus on higher learning institutions. This is the most recent framework with a focus on African institutions. In addition, the Lubua Framework emerged as the result of challenging the previous three frameworks and went through the validation process, as reported by Lubua and Pretorius (2019). Table 2 presents key elements of Lubua's framework.

Table 2: Lubua and Pretorius (2019) Cyber Security Policy Framework

Input	Description
Data Security	Every aspect of information security that will affect data on storage of transit

Internet and Network Services Governance	All aspects of the internet and network Governance
Use of Company Own Devices	All guidelines on the acceptable use of corporate ICT asset All guidelines on how to own devices are to be integrated into corporate LAN
Physical Security	Guidelines on how to ensure the physical security of Information Systems
Incidence Handling and Reporting,	Guidelines on how to handle and report incidents that would impact the business continuity
Monitoring and Compliance	Guidelines for using monitoring and control as a tool for ensuring business continuity
Policy Administration	Guidelines for administering the Information Security policy

Source: Lubua and Pretorius (2019)

4.2. Inputs from Review of the Existing Policies

In this study, we reviewed policies from eight organisations based in Tanzania to understand what they propose as the components of the policy. We also determined whether they have a new element to be added to the Lubua and Pretorius elements presented in Table 2. The key components of each policy are presented in Table 3.

Table 3: Inputs from Review of the Existing Policies

<i>Institution</i>	<i>Components of the policy</i>	<i>Input to the proposed framework</i>
Ardhi University (AU)	<ul style="list-style-type: none"> • Internet and email usage • Disaster management and training centre • recovery mechanisms such as backups • ICT hardware procurement guidelines • Software development and acquisition • Information management 	Internet and network services governance
Arusha Technical College	No input	No input
College of Business Education (CBE)	Hardware and Software management guidelines.	No Input
Eastern and Southern Africa Management Institute	No input	None
The Institute of Accountancy Arusha (IAA)	<ul style="list-style-type: none"> • Password management • Email use principles • Disaster recovery plan • Hardware and software management • Information handling 	Data and Information security
The Institute of Finance Management (IFM)	<ul style="list-style-type: none"> • Password Policy • Email use principles • Disaster recovery procedures • Hardware and software management Information handling	Data and Information security
The Open University of Tanzania (OUT)	<ul style="list-style-type: none"> • Disaster recovery for ICT services • Hardware and software management • Information handling 	Data and Information security
University of Dar es	<ul style="list-style-type: none"> • Disaster recovery plan for continuity of 	Data and Information

Salaam (UDSM)	business in case of a cyber-attack	security
	<ul style="list-style-type: none"> • Hardware and software management • Information handling. 	

Source: Research Data (2022)

According to Table 3, most elements of the examined policies are similar to those in the Lubua and Pretorius frameworks, except for a few. For example, at Ardhi University two components are added: ICT hardware procurement guidelines and software development and acquisition. Since both components suggest the process of acquiring ICT hardware or components, this study combines them to form one component to be used in the proposed framework. The new component is Acquiring hardware and software. On the other hand, the Institute of Accountancy Arusha, the Institute of Finance Management and the University of Dar Es Salaam had a common new component known as Information handling. In this regard, the study combines information handling and data security of Lubua’s framework to form a new component called Data and Information security. In addition, the study observed that Eastern and Southern Africa and Arusha Technical College had no ICT policy with tangible components. Because of the input from these policies, Table 4 presents the new framework structure.

Table 4: New framework structure – version 1

<i>Input</i>	<i>Description</i>
Data and Information handling	Every aspect of data and information security
Internet and Network Services Governance	All aspects of the internet and network Governance
Use of Company Own Devices	All guidelines on the acceptable use of corporate ICT asset All guidelines on how to own devices are to be integrated into corporate LAN
Physical Security	Guidelines on how to ensure the physical security of Information Systems
Acquiring hardware and software	All guidelines on how to acquire new hardware or software. It includes procurement or system development
Incidence Handling and Reporting	Guidelines on how to handle and report incidents that would impact the business continuity
Monitoring and Compliance	Guidelines for using monitoring and control as a tool for ensuring business continuity
Policy Administration	Guidelines for administering the Information Security policy

Source: Research Data (2022)

4.3. Inputs from the literature

We analysed the literature to understand the gap that exists between the framework presented in Table 2 and the literature. Table 5 presents inputs.

Table 5: Inputs from Review of Relevant Literature.

Author(s)	Addition to the structure
Lubua and Pretorius (2019),	<ul style="list-style-type: none"> • Policy review

(Semlambo, Almasi, Liechuka., 2022), (Hina & Dominic, 2018), (Mitra & Gilbert, 2012), (Patrick, Niekerk, & Fields, 2018)	<ul style="list-style-type: none"> • Users' awareness • stakeholders' Involvement in policy creation
Patrick, Niekerk, & Fields, 201), (Semlambo, Almasi, Liechuka., 2022), (Semlambo, Leichuka & Almasi, 2022),	<ul style="list-style-type: none"> • Training and awareness programmes on newly adopted ICT facilities (both hardware and software)
(Rajaonah, 2017), (Sapronov, 2020), (Mitra & Gilbert, 2012), (Patrick, Niekerk, & Fields, 2018), (Fouad, 2021)	<ul style="list-style-type: none"> • Awareness and training

Source: Research Data (2023)

Finding of the literature in Table 5 did not present something new. The components highlighted in Table 5, under the column known as “addition to the structure”, are confined within policy administration as per Table 4. Therefore, they don't change the structure in Table 4, but offer an explanation to one of its inputs. In summary, these elements include the need for frequent policy review, the need for developing ICT users' policy awareness, and the need to involve stakeholders in policy development. Because of this reason, this study presents Table 6 as its final structure representing the comprehensive Information Security Policy Framework.

Table 6: The Information Security Policy Framework

Input	Description
<i>Data and Information handling</i>	Every aspect of data and information security
<i>Internet and Network Services Governance</i>	All aspects of the internet and network Governance
<i>Use of Company Own Devices</i>	All guidelines on the acceptable use of corporate ICT asset All guidelines on how to own devices are to be integrated into corporate LAN
<i>Physical Security</i>	Guidelines on how to ensure the physical security of Information Systems
<i>Acquiring hardware and software</i>	All guidelines on how to acquire new hardware or software. It includes procurement or system development
<i>Incidence Handling and Reporting,</i>	Guidelines on how to handle and report incidents that would impact the business continuity
<i>Monitoring and Compliance</i>	Guidelines for using monitoring and control as a tool for ensuring business continuity
<i>Policy Administration</i>	Guidelines for administering the Information Security policy

Source: Research Data (2022)

5.0 CONCLUSION AND RECOMMENDATION

This study intended to develop a policy framework relevant to the public institutions of Tanzania. It used higher learning Institutions as its case for study. The following are the key policy components proposed for public institutions of Tanzania: Data and information handling, Internet and network services governance, the use of company-owned devices, physical security, guidance on acquiring hardware and software,

incident handling and reporting, monitoring and compliance, and policy administration. The study recommends the use of this framework in developing ICT policies with a cyber security perspective. The main limitation of the study is that it was mainly qualitative. A quantitative approach may add new value to the study. Also, the study used public higher learning institutions of Tanzania as the case for study. Therefore, additional studies can be done to include other organisations within Africa.

REFERENCES

- Abbasi, A., A. S.-N., Jalili, M., & Choi, S.-M. (2018). Enhancing Response Coordination Through the Assessment of Response Network Structural Dynamics. *PLOS ONE*, 1-17.
- Adler, D., & Grossman, K. L. (2001). *Establishing a Computer Incidence Reporting Plan*. Auerbatch Publications.
- Aiafi, P. R. (2017). The Nature of Public Policy Processes in the Pacific Islands. *Asia and Pacific Policy Studies*, 4(3), 451-466.
- Alexei, A. (2021). Network Security Threats to Higher Education Institutions. *Central and Eastern European e|Dem and e|Gov Days 2021* (pp. 321-333). Budapest, Hungary: Technical University of Moldova.
- Ali, R., & Zafar, H. (2018). A Security and Privacy Framework for e-Learning. *International Journal for e-Learning Security*, 7(2), 556-566.
- Alinaghian, R., Rahman, A. A., & Ibrahim, R. (2011). Information and Communication Technology (ICT) Policy; Significances, Challenges, Issues and Future Research Framework. *Australian Journal of Basic and Applied Sciences*, 5(12), 963-969.
- Almazán, D. A., Tovar, Y. S., & Quintero, J. M. (2017). Influence of Information Systems on Organizational Results. *ScienceDirect*, 62, 321-338.
- Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, 124(1), 691-697.
- Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone Users: Understanding How Security Mechanisms are Perceived and New Persuasive Methods. *PLOS ONE*, 1-35.
- Apuke, O. D., & Iyendo, T. O. (2018, 12 4). US National Library of Medicine. Retrieved from NCBI: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6299120/>
- Asgary, A. (2016). Business Continuity and Disaster Risk Management in Business Education: Case of York University. *AD-minister*, 1, 49-72.
- Balčiūnė, L., Ramanauskaitė, S., & Cenys, A. (2019). Information Security Management Framework Suitability Estimation for Small and Medium

- Enterprise. *Technological and Economic Development of Economy*, 25(5), 1-19.
- Botezatu, B. (2019). *New Cyberattack Tactics Against Businesses Require Advanced Network Defenses*. Illinois: Security Magazine.
- Broadhurst, R. G., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2018). *Phishing and Cybercrime Risks in a University Student Community*. SSRN Electronic Journal, 1-28.
- Brodin, M., Rose, J., & Åhlfeldt, R.-M. (2015). *Management Issues For Bring Your Own Device*. European, Mediterranean & Middle Eastern Conference on Information Systems (pp. 1-12). Athens: (EMCIS2015).
- Bruijn, H., & Janssen, M. (2017). *Building Cybersecurity Awareness: The Need for Evidence-Based Training Strategies*. *Government Information Quarterly*, 34(1), 1-7.
- Cannoy, S., Prashant C. Palvia, & Schilhavy, R. (2006). *A Research Framework for Information Systems Security*. *Journal of Information Privacy & Security*, 1(1), 1-17.
- Charoen, D. (2014). *Password Security*. *International Journal of Security (IJS)*, 8(1).
- Chen, Y., & He, W. (2013). *Security Risks and Protection in Online Learning: A Survey*. *International Review of Research in Open and Distance Learning*, 11(5), 108-127.
- Chowdhury, I. A. (2015). *Issues of Quality in a Qualitative Research: An Overview*. *Innovative Issues and Approaches in Social Sciences*, 8(1), 142-162.
- Dar, W. M. (2016). *Cyber Security Challenges on Academic Institution and Need for Security Framework toward Institutions Sustainability Growth*. *Advances in Computational Research*, 159-183.
- Dawson, M. (2018). *Applying a Holistic Cybersecurity Framework for Global IT Organizations*. *Business Information Review*, 35(2), 60-67.
- Dey, D., Lahiri, A., & Zhang, G. (2015). *Optimal Policies for Security Patch Management*. *Inform Journal of Computing*, 1-11.
- Fouad, N. S. (2021). *Securing higher education against cyberthreats: from an institutional risk to a national policy challenge*. *Journal of Cyber Policy*, 6(2), 137-154.
- French, A. M., Guo, C., & Shim, J. (2014). *Current Status, Issues, and Future of Bring Your Own Device (BYOD)*. *Communications of the Association for Information Systems*, 191-197.
- Galinec, D., Možnik, D., & Guberina, B. (2017). *Cybersecurity and Cyber Defence: National Level Strategic Approach*. *Automatica*, 58(3).

- Guma, A., Mbabazi, P., Lawrence, N., & Andogah, G. (2017). Use of Mobile Devices by Students to Support Learning in Universities: A Case of MUNI University. *International Journal of Research in Engineering & Technology*, 69-80.
- Hazut, N. (2019). Top Challenges When Securing Cloud Services Today. *Illinois: Security Magazine*.
- Hina, S., & Dominic, P. D. (2018). Information Security Policies' Compliance: a Perspective for Higher Education Institutions. *Journal of Computer Information Systems*, 1-11.
- International Standard Organisation. (2018). ISO 27000 Standards. Geniva: ISO.
- Järveläinen, J. (2012). Information Security and Business Continuity Management in Interorganizational IT Relationships. *Information Management & Computer Security*, 20(5), 332-349.
- Jr, C. D. (2017). Changes in Free and Open Source Software Licenses: Managerial Interventions and Variations on Project Attractiveness. 8(11), 1-12.
- Jum, K. S., Raihan, D. M., & Clement, D. C. (2016). Role of ICT in Higher Educational Administration in Uganda. *World Journal of Educational Research*, 3(1), 1-10.
- Kahyaoglu, S. B., & Caliyurt, K. T. (2018). Cyber Security Assurance Process From the Internal Audit Perspective. *Managerial Auditing Journal*, 33(1).
- Korhonen, J. J., Hiekkänen, K., & Mykkänen, J. (2012). Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions. IGI Global.
- Krishnaveni, D., & Meenakumari, J. (2010). Sage of ICT for Information Administration in Higher Education Institutions – A study. - *International Journal of Environmental Science and Development*, 282-286.
- Kundy, E. D., & Lyimo, B. J. (2019). Cyber Security Threats in Higher Learning Institutions in Tanzania A Case Study of University of Arusha and Tumaini University Makumira. *Olva Academy – School of Researchers*, 2(3), 1-37.
- Lafti, M. J., & MacDonald, J. L. (2019). Monitoring Threat Actors. *SYDNEY: Australia Cyber Security Magazine*.
- Lewis, J. (2018). Economic Impact of Cybercrimes-No Slowing Down. Santa Clara-CA: McAfee. Retrieved August 6, 2018, from <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf>
- Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security Policy Framework and Procedural Compliance in Public Organisations. *Proceedings of the International Conference on Industrial Engineering and Operations Management* (pp. 1-12). Pilsen, Czech Republic: *Proceedings of the International Conference on Industrial Engineering and Operations Management*.

- Lubua, E. W., Semlambo, A. A., & Pritorius, P. D. (2017). Factors Affecting the Use of Social Media in Learning Process. *South Africa Journal of Information Management*, 1-7.
- Lundgren, B., & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics*, 25(3), 1-8.
- Maple, C. (2017). Security and Privacy in the Internet of Things. *Journal of Cyber Policy*, 2(2), 155-184.
- McDermott, Y. (2017). Conceptualising the Right to Data Protection in an Era of Big Data. *Big Data & Society*, 4(1).
- Mitra, T., & Gilbert, E. (2012). Have You Heard?: How Gossip Flows Through Workplace Email. *Proceedings of the Sixth International AAI Conference on Weblogs and Social Media* (pp. 242-249). Dublin, Ireland, Spain: The AAI Press,.
- Moran, J. (2018). The 5 Components Of A Successful Incident Response Program. *ITSP Magazine*.
- Morgan, H. (2021). Conducting a Qualitative Document Analysis. *The Qualitative Report*, 27(1), 64-77.
- Moses, S., & Rowe, D. C. (2016). Physical Security and Cybersecurity: Reducing Risk by Enhancing Physical Security Posture through Multi-Factor Authentication and other Techniques . *International Journal for Information Security Research (IJISR)*, 667-676.
- Mtebe Aron, J., & Kondoro, K. W. (2016). Using Mobile Moodle to Enhance Moodle LMS Accessibility and Usage at the University of Dar es Salaam. *IST Africa*. Durban, South Africa: IST Africa.
- Mulenda, L., & Godfrey, M. (2018). Security Awareness and Social Media Usage in Learning Institutions in Tanzania. A Case Study of Mzumbe. Morogoro: Mzumbe University.
- Nagunwa, T., & Lwoga, E. T. (2012). Developing eLearning technologies to implement competency based medical education : Experiences from Muhimbili University of Health and Allied Sciences Thomas Nagunwa Institute of Finance Management , Tanzania Edda Lwoga Muhimbii University of Health and. *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, 8(3), 7-21.
- National Institute of Technology and Standards (NIST). (2022, 11 28). Cyber Security Framework. Retrieved from NIST: <https://www.nist.gov/cyberframework>
- Nyaranda, Z. I. (2012). Challenges and Opportunities of Technology Based Instruction in Open and Distance Learning: A Comparative Study of Tanzania and China. *Proceedings and report of the 5th UbuntuNet Alliance annual conference* (pp. 130-145). *Proceedings and report of the 5th UbuntuNet Alliance annual conference*.

- Olalere, M., Abdullah, M. T., Mahmood, R., & Abdullah, A. (2015). A Review of Bring Your Own Device on Security Issues. *SAGE Open*, 1-11.
- O'Leary, B. b. (2014). *The Essential Guide to Doing Your Research Project*. SAGE.
- Olsen, B. M. (2008). The Role Of End-User Training In Technology Acceptance. *Review of Business Information Systems – Second Quarter 2008*, 12(2), 1-8.
- Otito, G. (2013). The Reality and Challenges of E-Learning Education in Africa: The Nigeria Experience. *International Journal of Humanities and Management Sciences (IJHMS)*, 1(3), 205-209.
- Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, 132-145.
- Patrick, H., Niekerk, B. v., & Fields, Z. (2018). Information Security Management: A South African Public Sector Perspective. *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, 14.
- Perry, R. (2019). *Data Intelligence Not as Security, but as Accountability*. Paris: CPO Magazine.
- Pima, J. M., Odetayo, M., Iqbal, R., & Sedoyeka, E. (2016). Investigating the Available ICT Infrastructure for Collaborative Web Technologies in a Blended Learning in Tanzania: A Mixed Methods Research. *The International Journal of Education and Development using Information and Communication Technology*, 12(1), 37-52.
- Rajaonah, B. (2017). A View of Trust and Information System Security Under the Perspective of Critical. *Revue des Sciences et Technologies de l'Information - Série ISI : Ingénierie*, 22(1), 109-133.
- Ruzgar, N. S. (2005). A Research on the Purpose of Internet Usage and Learning Via Internet. *The Turkish Online Journal of Educational Technology*, 4(4), 27-32.
- Sabbagh, B. A. (2019). *Cybersecurity Incident Response; A Socio-Technical Approach*. Kista: Stockholm University.
- Sapronov, K. (2020). *The Human Factor and Information Security*. Kaspersky.
- Security Magazine. (2019). *Organizations At Risk for Data Breaches: System Vulnerabilities Increase by 92 Percent*. Security Magazine.
- Semlambo, Almasi, Liechuka. (2022). Perceived Usefulness and Ease of Use of Online Examination System: A Case of Institute of Accountancy Arusha. *International Journal of Scientific Research and Management (IJSRM)*, 10(4), 851-861.
- Semlambo, Leichuka & Almasi. (2022). Facilitators' Perceptions on Online Assessment in Public Higher Learning Institutions in Tanzania; A Case Study of the Institute of Accountancy Arusha (IAA). *International Journal of Scientific Research and Management (IJSRM)*, 10(6), 34-42.

- Shojaie, B. (2018). Implementation of Information Security Management Systems Based on the ISO/IEC 27001 Standard in Different Culture. Hamburg: Universitat Hamburg.
- Solms, R. v., & Niekerk, J. v. (2013). From Information Security to Cyber Security. Sciencedirect, 97-102.
- Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2018). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, 1-9.
- Tanzania Communication Regulatory Authority. (2022). 2022 Quarterly Statistics Reports. Dar es Salaam: Tanzania Communication Regulatory Authority.
- URT. (2007). Information and Communication Technology (ICT) for basic Education. Dar es Salaam: Ministry of Education and Vocational Training (MoEVT).
- URT. (2018). Quarterly Communications Statistics. Dar es Salaam: Tanzania Communication Regulatory Authority.
- Valencia, A. V., & Cázares, M. d. (2016). Academic and Research Networks Management: Challenges for Higher Education Institutions in Mexico. International Journal of Educational Technology in Higher Education, 1-12.
- Vorakulpipat, C., Sirapaisan, S., Rattanalerdnusorn, E., & Savangsuk, V. (2017). A Policy-Based Framework for Preserving Confidentiality in BYOD Environments: A Review of Information Security Perspectives. Security and Communication Networks, 1-11.
- Yıldırım, M., & Mackie, I. (2019). Encouraging Users to Improve Password Security and Memorability. International Journal of Information Security, 18(6).