International Journal of Technology and Management

The Quality of Information Systems Security Policies in Addressing Security Challenges in Public Learning Institutions of Tanzania.

IJOTM
ISSN 2518-8623

Volume 8. Issue I
pp. 1-22, June 2023
ijotm.utamu.ac.ug
email: ijotm@utamu.ac.ug

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

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

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

Abstract

Information and data in our organisations must be protected from illegal access and associated threats. Traditionally, a comprehensive information systems security policy sets the required foundation for protecting data by directing system users on how they must behave and offering necessary controls. With this understanding, the current study determined the quality of security policies adopted by learning institutions in guiding users on the prudent use of information systems. The following institutions were included in the analysis; The Institute of Accountancy Arusha (IAA), The Institute of Finance Management (IFM). College of Business Education (CBE), University of Dar es Salaam (UDSM), Ardhi University (ARU), Arusha Technical College (ATC), Open University of Tanzania (OUT) and Eastern and Southern African Management Institute (ESAMI). This study was qualitative and descriptive. It compared the key themes of an information security policy with the actual policies of the selected organisation. The purpose was to know whether these critical policy elements are considered in sampled policies for learning institutions based in Tanzania. The comparison theme includes password management, email use principles, disaster handling and recovery, hardware and software management, and information handling. The study found that higher learning institutions in Tanzania have poor information system security policies. A harmonised policy framework is necessary to improve the quality of policies used in learning institutions in Tanzania.

Key words: *Information security, Security policy, Information systems, Security threats, Compliance.*

Introduction

Information systems security remains one of the critical concerns of modern organisations, including higher learning institutions (Alqahtan, 2017). An organisation's information and data must be protected from internal and external attacks for smooth operations and trustworthiness (Maple, 2017). This is possible by minimising systems' exposure to threats while addressing available vulnerabilities. In this regard, systems software and their infrastructure must be deployed clearly to meet the data confidentiality, integrity, and availability objectives, whether under storage or transit (Mubarak., 2016). Unfortunately, according to studies Williams (2021) and Kaspersky (2021), there is evidence of violating these key principles of information security. In another piece of evidence by the International Telecommunication Union (ITU) in 2020, half of all Internet users worldwide compromised their security at one time of their technology use.

According to evidence from different studies, these security breaches are costly. For example, the International Business Machine Cooperation (International Business Machines Corporation, 2021) suggests that the cost of a data breach is estimated to be US$ 3.92 million annually globally. Moreover, Williams (2021) supports this study, who said that the cost of attacks rises yearly. Because of this reason, it is important to address factors affecting information security worldwide carefully. The study by Alotaibi, Furnell and Clarke (2016) report human factors affecting information systems security. In addition, the study by Assefa and Tensaye (2021) identified technical factors as the cause for insecurity, while the study by Ofori, Anyigba, Ampong, Omoregie and Nyamadi (2020) suggested that the insecurity is caused by The best way to address these factors, is to guide the technology use different security policies and guidelines as supported by Alhogail (2015).

Given this context, it is unarguable that the information security policy is among the critical administrative tools for ensuring the security of data, information and network infrastructure. One of the reasons supporting this assertion is that the policy formulation process identifies all potential security risks and threats to the organisation (Flowerday & Tuyikeze, 2016). It is easy to address challenges known to you. In addition, the policy document sets controls necessary in addressing risk areas (Alotaibi, Furnell, & Clarke, 2016; Alqahtani, 2017). Therefore, the policy provides a comprehensive guide for the organisation to meet its security objectives. Nonetheless, not all security policies are comprehensive enough to guide their users, as suggested by Lubua and Pretorius (2019); therefore, security policies need to be revisited to meet emerging requirements.

This study evaluates the quality of information system security policies of selected higher learning institutions based in Tanzania. The standard of evaluation is based on extracts from frameworks by ISO/IEC 27000:2018 (2018), Qureshi (2011), Lubua and Pretorius (2019), and Zhaq (2022). The evaluation selected these frameworks because they went through the review process, which validates their purpose of existence. This evaluation is based on the following elements - password management, email use principles, disaster handling and recovery, hardware and software management, and information handling.

2.0 Literature review

This section presents the literature on the quality of information systems security policies. The key elements of the section include an overview of information systems security followed by the quality of information systems security policy.

2.1. Information systems security

Evidence shows that human activities are increasingly dependent on information systems for operations and decision-making (Almazán, Tovar, & Quintero, 2017). In Tanzania, the use of ICT is growing at a rate of 4.9 per cent per year (Tanzania Communication Regulatory Authority, 2022). Currently, the number of internet users in Tanzania is 50%, compared to 60% of the world population using the internet (International Telecommunication Union, 2021) It is indisputable that efficiency in the use of information systems requires a reliable security to enhance the performance of the organisation (Almazán, Tovar, & Quintero, 2017).

The reliability of information systems is possible if supporting infrastructure and associated resources are safe. Factors affecting information systems' security include human-related, technical and administrative factors (Alotaibi, Furnell, & Clarke, 2016). According to Williams (2021), necessary controls are needed to address the vulnerabilities caused by these factors, which generally affect information systems' security. Based on this information, this study defines information system security as measures and practices implemented to protect the confidentiality, integrity, and availability of information within an organisation's information systems. It protects digital and physical assets, including hardware, software, networks, data, and the people interacting with these systems.

2.2. The quality of information security policies

In this context, the word quality represents the degree of excellence that can be achieved through policy implementation (Semlambo, Lubua, & Mkude, 2022). In this study, the work quality refers to the degree of excellence to be achieved in securing information systems. In this regard, quality policy considers technological concerns arising fromew developments in the industry, including the new release of security threats (Lange, Solms, & Gerber, 2015). Ultimately, the policy must enable the organisation to achieve universal security objectives, including confidentiality, integrity and data availability. The study by Lubua and Pretorius (2019) identified eight quality areas of an Information Security policy. The study asserted that the policy must address areas such as data security, internet and network services governancec guide the use of company-owned devices, guidance on the physical security of equipment, incident handling and reporting, monitoring and compliance, and policy administration. The study by Taylor (2001) identified the following security quality areas - security accountability, network service policies, system policies, physical security, incident handling and response, acceptable use policies, and security training. Moreover, Travellers Indemnity Company (2018) suggested the following elements - data security, password management policy, governing internet usage, managing email usage, use of company-owned devices, use of private devices, social media, software copyright and licencing, and reporting security incidents. The similarity between these studies is that they all considered physical security, incident reporting and monitoring, and data security foundational in ensuring information security.

The current study views quality areas identified by these studies as important in ensuring the security of Information Systems. Therefore, the study summarised these quality elements to set a standard for evaluating the quality of information security policies in selected learning Institutions. Table 1 summarises evaluation elements.

Table 1: Information System Security Policy Quality Evaluation Aspects

IS Security Policy focus areas	*Sub Areas*
Password management	Locking workstation when idle
	Privacy in password use
	Password strength
	Password use period
	Attachments management
Email and internet use principles	Dealing with forwarded emails
	ICT department's level of responsibility in email management
	Managing access to external websites
	Guidelines on acceptable use of the Internet
	Managing social media use
	Guidelines on how to use own devices for official purposes
Disaster handling and recovery	Guidelines on offsite backup
	Guideline on how to manage disasters
Hardware and Software Management	Software licence management
	Guidelines for upgrading system software and hardware
	Managing software installation
	Guidelines on administrative issues
Information handling	Guidance on data ownership
	Guidance on Information sensitivity and classification
	Guidance on how to dispose of data and information

Source: Researchers 2023

3.0 Research methodology

The study used the document analysis method to examine the quality of information systems security policies in addressing security challenges. According to Morgan (2021), document analysis allows the researcher to interpret documents to give them voice and meaning concerning a certain evaluation issue. It includes classifying information into themes like in focus group discussions or interviews, coding of evaluation criteria and analysing the results (O'Leary, 2014). The document analysis process followed this procedure.

Document Selection

Documents meant for review are mainly information security policies used by higher learning institutions in Tanzania. Other cited documents are there to affirm assertions made by this study. In our study, eight (8) institutions were used as the case study. The institutions are the Institute of Accountancy Arusha (IAA), The Institute of Finance Management (IFM). College of Business Education (CBE), University of Dar es Salaam (UDSM), Ardhi University (ARU), Arusha Technical College (ATC), Open University of Tanzania (OUT) and Eastern and Southern African Management Institute (ESAMI These institutions were selected based on their similarities in terms of ownership and of the fact that they share a common public ICT infrastructure; because they have a common Internet Service Provider (ISP). In all these organisations, the government has a stake.

In general, Tanzania has 582 higher learning institutions, of which only 212 are public higher learning institutions (URT, 2020) these eight institutions were purposively selected because their characteristics represent the rest of the population. The list includes Universities and technical institutions. Table 2 presents the institutions used in this study.

Table 2: Cases for Study

No	*Institution Name*	*Websites*	*Year ofPolicy Adoption*	*Yea of last Policy review*
01	Ardhi University (ARU)	https://www.aru.ac.tz	2019	2019
02	Arusha Technical College (ATC)	https://www.atc.ac.tz		
03	College of Business Education (CBE)	https://www.cbe.ac.tz	2020	2020
04	Eastern and Southern African Management Institute (ESAMI)	https://www.esamiafrica.org		
05	Institute of Accountancy Arusha (IAA)	https://iaa.ac.tz	2018	2022
06	Institute of Finance Management (IFM)	https://ifm.ac.tz	2012	2017
07	The Open University of Tanzania (OUT)	https://www.out.ac.tz	2014	2019
08	University of Dar es Salaam (UDSM)	https://www.udsm.ac.tz	2005	2019

Source: Researchers (2023)

Type of data and data collection procedures

The first step of the data collection process was to obtain the information security policy documents for all eight sample institutions. This was followed by reviewing the documents while relating them to sub-areas established in Table 1 for coding purposes. The information extracted was whether or not the element was found in the policy. Table 3 presents the summary of data extracts. If the element id found, it is coded as "yes", if not, it is coded as "no"

Table 3; Information System Security Policy Quality Evaluation Aspects

IS Security Policy focus	*Sub Areas*	*Code: Yes or No*

areas		
Password management	Locking workstation when idle	YES
	Privacy in password use	YES
	Password strength	NO
	Password use period	YES
	Extended use of passward	NO
Email and internet use principles	Attachments management	YES
	Dealing with forwarded emails	YES
	ICT department's level of responsibility in email management	YES
	Managing access to external websites	YES
	Guidelines on acceptable use of the Internet	YES
	Managing social media use	YES
	Guidelines on how to use own devices for official purposes	YES
Disaster handling and recovery	Guidelines on offsite backup	YES
	Guideline on how to manage disasters	YES
Hardware and Software Management	Software licence management	YES
	Guidelines for upgrading system software and hardware	YES
	Managing software installation	YES
	Guidelines on administrative issues	YES
Information handling	Guidance on data ownership	YES
	Guidance on Information sensitivity and classification	YES
	Guidance on how to dispose of data and information	

Source: Researchers (2023)

Data Analysis

This study intended to determine whether local ICT security-related policies meet minimum standards for the security of data and associated infrastructure. Sub-areas identified and coded in Table 3 were studied for each policy to see whether they are well covered. The study shows the similarity and differences in covering such sub-areas for each aspect. Overall, this study is descriptive. The magnitude at which all policies meet quality elements (for each element) was obtained through tallying inputs for each element from all policies.

4.0 Findings and Analysis.

This study evaluated the quality of information systems security policies among selected public higher learning institutions in Tanzania. The evaluation is guided by the framework in Table 1 and Table 3. The following aspects of evaluation are included: password management, email and internet use principles, disaster handling and recovery, hardware and software management, and information handling. Findings are presented in the next part.

i.) Password Management

Password management is used among the variables for evaluating the quality of information system security policies in this study. Accidentally password exposure violates privacy principles during data storage or communication. This variable includes locking the workstation when idle, maintaining password privacy, providing guidance on acceptable password strength, and providing guidance on password lifespan. Table 4 summarises the descriptive results of the evaluation.

Table 4: Evaluation of Password Management

Variable	Compliance Issue		No. of Non-compliance Issues	
	Freq.	Perc.	Freq.	Perc.
Locking work station when idle	1	12.5%	7	87.5%
Privacy in password use	2	25%	6	75%
Password strength	0	0%	8	100%
Extended use of default passwords	0	0%	8	100%

Source: Researchers 2022

Locking the Workstation when Idle

Findings show most policies do not give enough attention to the issue of locking workstations when idle. Only one (1) policy out of eight (8) is compliant. Therefore, computers are left vulnerable because they are unlikely to be accessed by unintended people, even within the organisation. The single institution compliant for this subcategory was a long-established institution with an ICT policy since 2012 that last updated its ICT policy in 2017. Their policy emphasises that when users leave their desks for any length of time, they must lock out of the workstation or lock the screen of their workstation.

Privacy in Password Use

Privacy in password use is discussed in two (2) policies out of eight (8). Thus, only 25% of all policies chosen for the case of the study are compliant with password privacy. This can result in security vulnerabilities if the ICT facilities of the organisation are not properly protected through appropriate passwords. Within the two policies, similarities in password privacy exist only in one account, where both policies restrict users from sharing personal passwords. The other policy is more detailed and continues to emphasise the following: access to institutions' ICT facilities through passwords; use of unique usernames and passwords; the automatic issue of passwords by the institute; and restriction on illegally bypassing passwords through tools such as password breakers. Both policies are from institutions, one established in 2018 and reviewed in 2022, and the other established in 2012 and reviewed in 2017. Though these two institutions have policies about password privacy, the emphasis is not enough as important password privacy key points are left behind.

Password Strength

Password strength is another feature of a password used to protect information security in an organisation. This subcategory has not been found in any of the policies chosen for the case of the study, which resulted in 0% compliance.

The Use of Default Password

This sub-category had 0% compliance as it did not reflect any policy in the chosen case for study. Applications are created to speed up setup time and offer clients the best possible user experience, particularly when the administrator must install the application on various devices one after the other. This is illustrated by the default passwords used in this study, which are simple to remember and can be used on numerous devices. For instance, the majority of programmes use the default passwords "password," "admin," "dba," et.

ii.) Email Use Principles

Email use principles are among the key variables for evaluating the quality of information system security policies as established through the framework in Table 1. Categories explaining this variable include attachment management; dealing with forwarded emails; the IT department's level of responsibility in email management; managing access to external websites; guidelines of acceptable use of the internet; managing social media use; and guidelines on how to use one's own devices for official use. Table 5 summarises the results of the evaluation.

Table 5; Evaluation of Email Use Principles

Variable	Compliance Issues		No. of Non-compliance Issues	
	Freq.	Perc.	Freq.	Perc.
Attachments management	2	25%	6	75%
Dealing with forwarded emails	*1*	*12.5%*	*7*	*87.5%*
IT department's level of responsibility in email management	6	75%	2	25%
Managing access to external websites	1	12.5%	7	87.5%
Guidelines on acceptable use of the internet	5	62.5%	3	37.5%
Managing social media use	1	12.5%	7	87.5%
Guidelines on how to use own devices for official purposes	1	12.5%	7	87.5%

Source: Researchers 2022

Attachments Management

This subcategory received 25% compliance, where only two (2) policies out of eight (8) had notes concerning attachment management. Both institution policies emphasised the size of email with an attachment that can be sent and received via the exchange servers of the institution, which should not be more than 100MB to avoid network traffic. One of the policies was created in 2018 and reviewed in 2022, while the other was created in 2012 and reviewed in 2017. To avoid information system security incidences such as phishing attacks where malicious people attach links and other attachments in emails compromise the organisation's information system.

Dealing with Forwarded Emails

This subcategory appeared in only one (1) policy out of eight (8). The policy only explains the right of the institute to inspect, monitor, and disclose the content of any email created, sent, received, or forwarded using the institute's computer network or email systems. The policy was created in 2012 and reviewed in 2017.

IT Department's Level of Responsibility in Email Management

This sub-category had a higher compliance level of 65% (Table 5). However, the complying institutions' emphasis on the IT department's level of responsiveness in email management differs in their policies. Out of six (6) compliant institutions, four only mention the mandatory use of institutions' internal email services for all office use and management of internal and external emails, spam email and limitations in attachment size. But two institutions have approximately managed to capture all the important aspects of email management, such as the content of the email to avoid sending and receiving offensive email at work; restrictions on the forwarding of junk and spam emails; restrictions on using other email accounts and data files; restrictions on using email to send text, images or videos that are considered illegal or indecent, such as pornographic content; restrictions on sending emails containing viruses; restrictions on sending group emails unless with proper authorisation; and lastly, maintaining the email of retired staff is restricted for not more than one (1) year.

Managing Access to External Websites

This sub-category had a 12.5% compliance level, where only one (1) policy out of eight (8) policies contained notes on managing access to external websites. The compliance policy was developed in 2012 and updated in 2017. The policy note emphasised the importance of not using the internet provided by the institute to gain unauthorised access to other systems or websites. The remaining policies talked about websites only concerning the institution's website, disregarding anything related to accessing external websites.

Guidelines on Acceptable Use of the Internet

This sub-category had a 62.5% compliance level, where five (5) out of eight (8) policies had notes about acceptable internet use. These notes about the acceptable Internet use were similar to almost all of these five institutions. They cover topics such as internet service providers, where they are all required to use government internet service providers due to their status as public institutions

Managing Social Media Use

Only one (1) policy complied with this sub-category out of eight (8) policies. The university policy was developed in 2014 and reviewed in 2019. The policy notes emphasise two things; using social media to inform the public about university services and using social media as a data collection tool for user opinion on improving university services. Though this is the only policy with a note on managing social media use, the note is not clear enough on how these social media can be managed to protect the security of the university information system.

Guidelines on How to Use Own Devices for Official Purposes

The use of personal devices for official purposes was covered in only one (1) policy out of eight (8) under the category of Bring Your Own Device (BYOD). The institution's policy was created in 2018 and reviewed in 2022. The policy notes state that device owners must take personal responsibility to prevent data theft and loss, keep the information confidential when necessary, maintain the integrity of data and information and accept responsibility for any software used or downloaded to their devices. One of the restrictions to handling BYOD practice vulnerabilities is providing users with temporary identification cards (ID) or log-in credentials to access the institute's internet and network connection.

iii.) Disaster Handling and Recovery

Disaster handling and recovery are among the key variables for evaluating the quality of information system security policies as established through the framework in Table 1. Categories explaining this variable include guidelines on offsite back-ups and how to manage disasters. Table 6 summarises the results of the evaluation.

Table 6; Evaluation of Disaster Handling And Recovery

Variable	Compliance Issue		No. of Non-compliance Issues	
	Freq.	Perc.	Freq.	Perc.
Guidelines on offsite backup	2	25%	6	75%
Guideline on how to manage disasters	1	12.5%	7	87.5%

Source: Researchers 2022

Guidelines on Offsite Backup

Backup and restoration policies aim to give the institute's vital data secure storage and a way to restore the data in case of system failure. Additionally, it enables prompt restoration of stored data in case of a catastrophe or system failure. This sub-category had 25% of compliance, where only two (2) out of eight (8) policies had notes on offsite backup. The policies set out what kind of backup should be done daily and what kind of data backup should be done weekly. Policies have other backup procedures such as who is responsible for conducting back-ups, where and how to store backup media and label them accordingly, and disposal of unrequired backup media.

Guideline on how to Manage Disasters

Only one (1) policy out of eight (8) chosen for the case study had notes on managing the disaster. The complaint policy was developed in 2014 and reviewed in 2019. The university policy emphasises how to handle disasters only covers issues like having a disaster recovery plan, having onsite and offsite data backup, having physical and logical security for all university ICT infrastructures, and the usability of ICT devices with appropriate authentication and power backup, and fire extinguishing.

iv.) Hardware and Software Management

Hardware and Software Management is among the key variables for evaluating the quality of information system security policies as established through the framework in Table 1. Categories explaining this variable include software license management, guidelines for updating system software and hardware, managing software installation and guidelines for administrative issues. Table 7 summarises the results of the evaluation.

Table 7; Evaluation of Hardware and Software Management

Variable	Compliance Issue		No. of Non-compliance Issues	
	Freq.	Perc.	Freq.	Perc.
Software licence management	5	62.5%	3	37.5%
Guidelines for upgrading system software and Hardware	5	62.5%	3	37.5%
Managing software installation	5	62.5%	3	37.5%
Guidelines on administrative issues	5	62.5%	3	37.5%

Source: Researchers 2022

Software Licence Management

This sub-category had 62.5% compliance, where five (5) out of eight (8) institution policies had notes on software licence management. The compliance policies focus on the use of legal-licensed software and restrict the use of pirated software; the use of software that complies with the institution's and national as well as international standards; regular updating of software to keep up with changes in technology and business environment; and prioritise the use of open-source software. Noncompliance with such guidelines by some institutions has resulted in public higher learning institutions using outdated software, such as Windows XP and MS Office 2007, which is no longer supported by its vendor (Microsoft). Some of the software is not licensed, so the user cannot have full access to all software features, leading to information system security vulnerabilities.

Guidelines for Upgrading System Software and Hardware

System software and hardware need regular updates to keep up with technological change and stay competitive in the business environment (Yang, Hosseinian-Far, Jraisat, & Rangaswamy, 2021). This sub-category received 62.5% compliance with five (5) policies out of eight (8) discussed upgrading system software and hardware. Some policy notes were too narrow, only discussing compliance with standards when purchasing new software and hardware. Other policies had a bit more notes, such as compliance with national and international standards, warranty and guarantee certificates of at least one (1) year upon the purchase of new hardware and software.

Managing Software Installation

This sub-category received 62.5% compliance with five (5) policies out of eight (8) having notes discussing software installation management. The compliant policies discussed the installation of software with compliance to institutional standards as well as national and international standards, the responsibilities of who is responsible for the installation and updating of software, and restrictions on the installation of unlicensed software.

Guidelines on Administrative Issues

This sub-category had 62.5% compliance where five (5) out of eight (8) policies contained guidelines on administrative issues such as responsibilities of software and hardware purchase, compliance with different national and international as well as institute standards, compliance with user requirements and authorisation of use of licenced software.

v.) Information Handling

Information handling is among the key variables for evaluating the quality of information system security policies as established through the framework in Table 1. Categories explaining this variable include guidance on data ownership, information sensitivity and classification, and how to dispose of data and information. Table 8 summarises the results of the evaluation.

Table 8; Evaluation of Information Handling

Variable	Compliance Issue		No. of Non-compliance Issues	
	Freq.	Perc.	Freq.	Perc.
Guidance on data ownership	4	50%	4	50%
Guidance on Information sensitivity and classification	1	12.5%	7	75%

Guidance on how to dispose of data and information	1	12.5%	7	75%

Source: Researchers 2022

Guidance on Data Ownership

The sub-category of data ownership had a compliance level of 50%, where four (4) of the policies in all eight (8) policies chosen for the study had notes on data ownership. The policies in the subcategory contained only a few notes on data ownership, such as security of institution data and individual data in the institution network, regular review and audit of information systems to ensure that they are secure, available, easy to use, and meet the requirements of appropriate interoperability and data exchange mechanisms, and mechanisms to ensure backup in the event of data loss through onsite and offsite backup.

Guidance on Information Sensitivity and Classification

Only one (1) policy out of eight (8) reviewed policies had notes on information sensitivity and classification. Though the notes in this policy were too brief, simply explaining data classification to control access in a shared institution network. This study found that policies have minimal notes on information categorisation based on public, protected, and confidential information. This has resulted in ICT users disregarding what information should be shared with whom and where, such as discussing office-related issues on social networking sites such as WhatsApp groups (as explained in the previous sub-category). Based on the fact that there is minimal management of information in public higher learning institutions.

Guidance on How to Dispose of Data and Information

This sub-category had a 12.5% compliance level, where only one (1) institution out of eight (8) chosen cases for the study had notes on how to dispose of institute data and information. The compliance policies focused on disposing of data and information based on government policies, rules, and regulations to ensure no institutional data remains on the device in case the device is sold to a third party. The study found that policies have minimal notes on the disposal of work documentation and office records. Also, there is no indication of how often this needs to be done, and there is no specification on how to dispose of physical and digital documents.

5.0. Discussion of Findings

This section discusses the findings presented in section 4 (findings and analysis). The following aspects of evaluation are included: password management, email use principles, disaster handling and recovery, hardware and software management, and information handling. A discussion of each of these elements is presented in the next part.

i.) Password Management

The findings and analysis show that 7 out of 8 information system security policies from the selected institutions do not compile to the four subcategories of locking the workstation during idle and privacy in password use. This leaves these institutions vulnerable to different information system security threats from anyone who can use these unattended workstations maliciously. Yldrm and Mackie (2019), IAU (2020) and Charoen (2014) discussed using software to analyse the strength of passwords and stressing the importance of password memorability. Research has found that password strength is more secure than normal passwords, and this has not been found in any of the 8 institutions selected for this study. Additionally, using default passwords over an extended period can lead to information system security vulnerabilities as they become known by all users and can be used by unauthorised personnel to gain access to secure organisation information and data.

ii) Email Use Principles

The most important details in Email use principles are attachment management, dealing with forwarded emails, IT Department's Level of Responsibility in Email Management, and Managing access to external websites. Attachment management has 6 non-compliant levels, dealing with forwarded emails has 7 non-compliant levels, IT Department's Level of Responsibility in Email Management has 2 non-compliant levels, and Managing access to external websites has 7 non-compliant levels. These policies were developed in 2012 and renewed in 2017 and 2022 respectively. The most important details in this category are that 5 of the information system security policies from case institutions had poor compliance levels in this subcategory and that managing social media users had a poor complement level due to different information system security threats and vulnerabilities from using social media in learning institutions' networks. Additionally, Majid and Kouser (2019) listed the causes of risk in social media, such as forgetting to log out, logging in on foreign websites, clicking on enticing ads, using third-party apps, using common passwords, clicking on malicious links and using virtual private networks (VPN).

To have proper information system security in an organisation, policy should have clear notes on how social media use in the organisation will be managed. Social networking sites can bring advantages to learning environments, but they can also harm productivity as emphasised by other researchers such as Broadhurst, Skinner, Sifniotis, Matamoros-Macias and Ipsen (2018), Chaudhry, Chaudhry and Rittenhouse (2016) and Gupta, Arachchilage and Psannis (2018). Public higher learning institutions need information system security policies to address the appropriate use of social networking sites and restrictions on some sites that can damage an organisation's core objectives. Guidelines on using own devices for office purposes had a poor compliance level. Higher learning institutions' ICT policies must evaluate various processes and procedures, such as online assessment and examination systems, mobile learning technologies, and video conferencing facilities. BYOD restrictions must be specified to protect users and the institute from potential threats. ICT/ Information System security policies must provide information on how users can protect themselves from such vulnerabilities (Jahanbakhsh, Amini-Rarani, Tahmasebian, & Shahbazi, 2020).

iii) Disaster Handling and Recovery

This study assessed the effectiveness of information system security policies, including recommendations for offsite data backups and protocols for handling unforeseen catastrophic events. It found that more attention needs to be given to the importance of regular offsite backup to save data from different kinds of disasters.

Guidelines on managing disaster had 7 non-compliant kevels out of 8 information system security policies from the case institutions. These policies should clearly state how disasters caused by natural occurrences or humans can be handled and their specific procedures for dealing with the situation. To ensure confidentiality, integrity, and availability of institutional data, it is important to have a regular and reliable offsite backup through appropriate processes and procedures, which must be well defined within policies to avoid any information system security incidences. Other researchers, including Sharma and Singh (2012). These disasters should be documented and well-studied to have measures in place so that they do not repeat in the future and give a chance to other institutions to learn from them and protect themselves from facing the same challenges (Asgary, 2016).

iv) Hardware and Software Management

Evaluating the effectiveness of information system security policies involves examining hardware and software management. In the subcategory of software license management, 3 non-compliant out of 8 information systems security policies were reviewed from the case institutions. Other researchers highlighted issues such as user requirements and feedback, user recommendations, guidelines on yearly maintenance, system architecture and design schemes, storage and indexing techniques, query processing and optimisation, and transaction processing in platforms with new hardware (Wei Pan, Zhang, & Weng, 2018). Institution policies should clearly state hardware and software management for the appropriate use of ICT infrastructures and emphasise appropriate training and awareness programmes before introducing new hardware or software (Yang, Hosseinian-Far, Jraisat, & Rangaswamy, 2021). This study found that managers are often excluded from committees formulating ICT and information system security policies in Tanzania's public higher learning institutions.

Employees' involvement in creating these policies is poor and is not shared with all employees. To clearly understand potential security areas, all employees must be involved in the policy creation process (Glaspie & Karwowski, 2018). Employees should be involved in information system security policies to motivate security habits and eliminate risk behaviours. Informal guidelines are used instead of policies but are inadequate against information security challenges due to stakeholders not being involved enough (Astakhova, 2016; Robinson, 2019). Regular training and awareness programmes should be provided, but they have no application.

v) Information Handling

Assessing the effectiveness of information system security policies involves considering the handling of information. The evaluation results are summarised in Table 8. Guidance on data ownership had 4 noncompliant levels out of 8 information system security policies reviewed by the case institutions. Guidance on information sensitivity and classification had 7 non-compliant levels out of 8 information systems security policies reviewed by the case institutions. Data disposal methods should centre on data anonymisation, deletion, crypto shredding, degaussing, and destruction (Kablawi, 2022. As explained by other researchers, these notes were too minimal to cover all the necessary possession and responsibility of institutional data, as explained by other researchers (Al-Khouri, 2002; Fadler & Legner, 2022). Public higher learning institutions' policies need clear and well-explained guidelines on ownership of institutional data and individual data within institutional information systems to ensure information system security. The management of these institutions needs to maintain good information system security policies and the security of the information by categorising information based on confidential, restricted, and public. Furthermore, awareness of who can access what information within and outside the organisation is essential (Lamp, 2011).

6.0 Conclusion and Recommendations.

Conclusion

The findings of this study showed that information systems security policies of public higher learning institutions do not have enough notes on how to manage login credentials to their ICT infrastructures. This includes locking the workstation while idle, privacy in password use, password strength and extended use of default passwords. Although the IT department level of responsibility in email use principles is satisfactory to most public higher learning institutions, other email management principles like attachment management, dealing with forwarded emails, managing access to external websites, guidelines on acceptable use of the internet, managing social media use and guideline on how to use one device for office purposes have not been well addressed and need considerations for improvement. Disaster handling and recovery are also overlooked by most public higher learning institutions' information system security policies/ this includes insufficient notes on policy regarding guidelines on offsite backup and how to manage the disaster. Regarding hardware and software management, this study found that most public higher learning institutions' information system security policies comply with most guidelines. However, improvement is needed as some institutions comply poorly with the guidelines. Lastly, there is poor compliance in information handling and a need for more improvements.

Recommendations

Based on the findings of this policy evaluation, this study concludes that the quality of policies is still poor. In essence, there is no one perfectly compliant policy. This suggests a low quality to organisations' security policies. This level of quality sets a poor security foundation, resulting in a security breach. Since this is a policy-based study, we make the following recommendations: -

i. Institutions must engage in the use of harmonised frameworks in developing their policies to address observed challengesThere must be a good level of policy awareness in the team that develops the policy.
ii. The policy development must engage different stakeholders to use their knowledge and opinions, in policy development extensively
iii. This study recommends using a harmonised, standardised, well-developed information system security policy framework.

The study recommended a regular review of policies since they are subjected to a regular changes. The recommended time is usually at the maximum threshold of 3 years.

References

Alghamdi, A. (2020). Security Lock systems: From Problem Statement to System Design Name of the Author. Umm Al-Qura University, Makkah, Saudi Arabia, 1-7.

Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organisations. Journal of Theoretical and Applied Information Technology, 78(2), 201-211.

Al-Khouri, A. M. (2002). Data Ownership: Who Owns 'My Data'? international journal of management & information technology, 2(1), 1-8.

Almazán, D. A., Tovar, Y. S., & Quintero, J. M. (2017). Influence of Information Systems on Organizational Results. ScienceDirect, 62, 321-338.

Alotaibi, M., Furnell, S., & Clarke, N. L. (2016). Information Security Policies: A Review of Challenges and Influencing Factors. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 1-7). Plymouth, UK : ICITST.

Alqahtan, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. 4th Information Systems International Conference (pp. 691-697). Bali - Indonesia: ScienceDirect.

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. 4th Information Systems International Conference (pp. 691-697). Bali, : ISICO.

Apuke, O. D., & Iyendo, T. O. (2018). University Students' Usage of the Internet Resources for Research and Learning: Forms of Access and Perceptions of Utility. National Library of Medicine, 4(12).

Arbanas, K., & Hrustek, N. Ž. (2019). Key Success Factors of Information Systems Security. Key Success Factors of Information Systems Security, 43(3), 131-144.

Asgary, A. (2016). Business Continuity and Disaster Risk Management in Business Education: Case of York University. AD-minister, 1, 49-72.

Assefa, T., & Tensaye, A. (2021). Factors influencing information security compliance: an institutional perspective. College of Natural and Computational Sciences, Addis Ababa University, 44(1), 108–118.

Awolusi, F. (2012). The Impacts of Social Networking Sites on Workplace Productivity. ournal of Industrial Technology, 28(1), 1-6.

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.

Charoen, D. (2014). Password Security. International Journal of Security (IJS), 8(1), 1-14.

Chaudhry, J. A., Chaudhry, S., & Rittenhouse, R. G. (2016). Phishing Attacks and Defenses. International Journal of Security and its Applications, 10(1), 247-256.

Chen, X., Chen, L., & Wu, D. (2011). Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. Journal of Computer Information Systems, 58(4), 1-13.

Edga, T. W., & Manz, r. O. (2017). Research Methods for Cyber Security.

Eliringia, K. H. (2017). Effects of Social Networking on Employees Performance A Case of Reginal Secratariat - Mara Region. Morogoro: Mzumbe University.

Fadler, M., & Legner, C. (2022). Data Ownership Revisited: Dlarifying Data Accountabilities in Times of Big Data and Analytics. Journal of Business Analytics , 123-139 .

Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., & Meitern, M. (2016). Advancing Cybersecurity Research and Education in Europe. New York: Association for Computing Machinery.

Gardner, B., & Thomas, V. (2014). Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats 1st Edition. elsevier, 1-16.

Ghavifekr, S., & Rosdy, W. A. (2015). Teaching and Learning with Technology: Effectiveness of ICT Integration in Schools. International Journal of Research in Education and Scienc e, 1(2), 175-191.

Gupta, B. B., Arachchilage, N. A., & Psannis, K. E. (2018). Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions. Telecommunication Systems, 67(5), 1-21.

Heerden, D. v., & Goosen, L. (2018). Information Systems to Support Learning in an Information and Communication Technology Module. International Conference Europe Middle East & North Africa on Information Systems and Technologies to support Learning 2018 (EMENA-ISTL 2018) (pp. 1-10). International Conference Europe Middle East & North Africa on Information Systems and Technologies to support Learning 2018 (EMENA-ISTL 2018).

Hina, S., & Dominic, D. D. (2018). Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems, 60(3), 1-11.

IAU. (2020). The Impact of COVID-19 on Higher Education Worldwidel Resources for Higher Education Institutions. International Association of Universities.

International Business Machine Cooperation (IBM). (2021). Cost of Data Breach Report. IBM.

International Business Machines Corporation. (2021). Why Data Security is Vital for the Well-Being of Any Enterprise Today. New York: IBM.

International Telecommunication Union. (2020). Computer Security Incident. Geneva, Switzerland: ITU. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Computer%20Incident%20Handling%20.pdf

International Telecommunication Union. (2021). Statistics. Geneva. Switzerland: International Telecommunication Union.

ISO/IEC 27000:2018. (2018). Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary. ISO/IEC.

Jahanbakhsh, M., Amini-Rarani, M., Tahmasebian, S., & Shahbazi, M. (2020). Policy Making for Applying Bring Your Own Device Approach in COVID-19 Pandemic: A Perspective. Vesnu Publicationss.

Jothi, S., Neelamalar, & Prasad, S. (2011). Analysis of Social Networking Sites: A Study on Effective Communication Strategy in Developing Brand Communication. Journal of Media and Communication Studies, 3(7), 234-242.

Kablawi, B. (2022). Why (and How to) Dispose of Digital Data. ISACA.

Kaspersky. (2021). Top Ransomware Attacks of 2020. Moscow-Russia: Kaspersky.

Knierem, B., Zhang, X., Levine, P., Breitinger, F., & Baggili, I. (2018). DigitalComons @ New Haven . An Overview of the Usage of Default Passwords, 1-6.

Kothar. (2004). Research Methodology; Methods and Techiques. New Delhi: New Age International Publishers.

Lamp, J. W. (2011). Information Categorisation: an Emergent Approach. Melbourne.: The University of Melbourne.

Lange, J. d., Solms, R. V., & Gerber, M. (2015). Better Information Security Management in Municipalities. IST-Africa (p. 1+10). Malawi: IST-Africa .

Lohani, S. (2019). Social Engineering: Hacking into Humans. International Journal of Advanced Studies of Scientific Research,, 4(1), 385-395.

Lubua, E. W., & Pretorius, P. D. (2019). Ranking Cybercrimes Based on Their Impact to Organisations' Welfare. THREAT Conference Proceedings (pp. 1-11). Johannesburg: THREAT Conference Proceedings.

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.

M. Yıldırım & I. Mackie. (2019). Encouraging Users to Improve Password Security and Memorability. International Journal of Information Security, pages741–759.

Majid, I., & Kouser, S. (2019). Social Media and Security: How To Ensure Safe Social Networking. International Journal of Humanities and Education Research, 1(1), 36-38.

Maple, C. (2017). Security and privacy in the internet of things. Journal of Cyber Policy, 2(2), 155-184.

Metalidou, E., Marinagi, C. C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. A. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 147, 424-428.

Mubarak., S. (2016). Developing a theory-based information security management framework for human service organisations. Journal of Information, Communication and Ethics in Society, 14(3), 254-271.

Nordström, T., Söderström, M., & Hanseth, O. (2000). Business Development in IT-dependent organisations. Proceedings of IRIS 23. Laboratorium for Interaction Technology, (pp. 1-12). rollhättan Uddevalla,: University of Trollhättan Uddevalla,.

Norsaremah, S., Hussein, R., Norshidah, M., & Umar, A. (2013). An Empirical Study of the Factors Influencing Information Disclosure Behaviour in Social Networking Sites. Advanced Computer Science Applications and Technologies (ACSAT) (pp. 181-185). International Conference on, pp.

Ofori, K. S., Anyigba, H., Ampong, A., Omoregie, O. K., Nyamadi, M., & Fianu, E. (2020). Factors Influencing Information Security Policy Compliance Behavior. Hershey, Pennsylvania: IGI Global is prohibited.

O'Leary, B. b. (2014). The Essential Guide to Doing Your Research Project. SAGE.

Pal, O., & Alam, B. (2017). Cyber Security Risks and Challenges in Supply Chain. International Journal of Advanced Research in Computer Science, 5, 662-666.

Retnowardhani, A., Diputra, R. H., & Triana, Y. S. (2019). Security Risk Analysis of Bring Your Own Device (BYOD) System in Manufacturing Company at Tangerang. Telecommunication Computing Electronics and Control, 17(2).

Robinson, S. C. (2019). Factors Predicting Attitude Toward Disclosing Personal Data Online. Journal of Organizational Computing and Electronic Commerce, 28(3), 214-233.

Sánchez, S. P., López-Belmonte, J., Moreno-Guerrero, A.-J., Reche, J. M., & Cabrera, A. F. (2020). Effect of Bring-Your-Own-Device Program on Flipped Learning in Higher Education Students. Susteinability, 12, 1-11.

Semlambo, A. A., Lubua, E. W., & Mkude, C. G. (2022). Factors Affecting the Security of Information Systems in Africa: A Literature Review.

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.

Sharma, K., & Singh, K. R. (2012). Online Data Back-up and Disaster RecoveryTechniques in Cloud Computing: A Review. International Journal of Engineering and Innovative Technology (IJE, 2(5), 249-254.

Simon, K., & Cheung, S. (2014). Information Security Management for Higher Education Institutions. Intelligent Data analysis and its Applications, 1, 11-19.

Siponen, M., Mahmood, A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.

Talebian, S., Mohammadi, H. M., & Rezvanfar, A. (2014). Information and communication technology (ICT) in higher education: advantages, disadvantages, conveniences and limitations of applying e-learning to agricultural students in Iran. ScienceDirect, 300-305.

Tanzania Communication Regulatory Authority. (2022). 2022 Quarterly Statistics Reports. Dar es Salaam: Tanzania Communication Regulatory Authority.

The National Council for Technical Education (NACTE). (2020). Registered and Accredited Institutions. Dar es Salaam: The National Council for Technical Education (NACTE).

The Public Procurement Act (410). (2013). The Public Procurement Act (410). Dar es Salaam: Goverment Printer.

Tinmaz, H., & Lee, J. H. (2019). A Perceptional Analysis of BYOD (Bring Your Own Device) for Educational or Workplace Implementations in a South Korean Case. Participatory Educational Research (PER), 5164.

V.Flowerday, S., & TiteTuyikeze. (2016). Information security policy development and implementation: The what, how and who. Computers & Security, 61, 169-183.

Väyrynen, K., Hekkala, R., & Wiander, T. (2012). Information Security Challenges of Social Media for Companies. uropean Conference on Information Systems (ECIS) (pp. 1-13). Barcelona, Spain: uropean Conference on Information Systems (ECIS).

Wei Pan, Z. L., Zhang, Y., & Weng, C. (2018). The New Hardware Development Trend and the Challenges in Data Management and Analysis. Springer, 3, 263–276.

Williams, S. (2021). Cyberattacks on Organisations Worldwide Surge 40% in 2021. newzealand : SecurityBrief.

Wismen, M., & Keller, C. (2017). implementation Of Information Security Policies in Public Organisations. Jonkoping University.

Yang, W. K., Hosseinian-Far, A., Jraisat, L. E., & Rangaswamy, E. (2021). Software License Audit and Security Implications. Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London. London: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London.

Zhaq, J. (2022, April 14https://hyperproof.io/resource/information-security-policy/). Hyperproof. Retrieved from Build Strong Information Security Policy: Template & Examples.