

International Journal of Technology and Management

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

IJOTM
ISSN 2518-8623
DOI: 10.67610/ijotm.8.1.001
Volume 8. Issue I
pp. 1-23, June 2023
ijotm.utamu.ac.ug
email: ijotm@utamu.ac.ug

Adam A. Semlambo
Department of Information and Communication Technology
The Open University of Tanzania
semlambo@gmail.com

Edison Wazoel Lubua (PhD)
Associate Professor
Department of Informatics
Institute of Accountancy Arusha

Catherine G. Mkude (PhD)
Department of Information and Communication Technology
The Open University of Tanzania

Abstract

Information and data in Higher Learning Institutions must be protected from attacks and secured from illegal access, unwanted interruptions, and unauthorised alteration or inhalation. Many institutions fall victim to such attacks due to weak information system security policies. Also, employees' disruption of these information system security policies can cause information technology vulnerabilities and lead to information security threats.

Through qualitative methodology, thematic and descriptive analyses were used to review ICT/ information system security policies to determine their quality in addressing information security challenges in public higher learning institutions in Tanzania. A sample of eight public higher learning institutions was used. Common themes included password management, email use principles, disaster handling and recovery, hardware and software management, and information handling. The study found that the security level of these elements varied among focused areas due to a need for more information system security policy awareness and compliance.

This study proposes using a harmonised information system security policy framework for all public higher learning institutions while maintaining good control through government agencies and appropriate training and awareness programs. The study also emphasises the need for policy review every four years so that these institutions' Information System Security policies remain current and proactive in their use/ Also to accommodate new technological changes that bring new information system security threats.

Key Words: Higher Learning Institutions, Information System Security, Information System security policy, Security Threat, Information Technology, Compliance.

Introduction

Information system 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 (Maple, 2017). This is possible through minimising exposure to threats. Therefore, systems and their infrastructure must be deployed with a clear focus on confidentiality, integrity, and data availability under storage or in transit (Mubarak., 2016). Unfortunately, evidence shows the violation of these principles of information security. For example, the study by Williams (2021) reports the release of 63 attacks every day worldwide. Kaspersky supports that report by estimating 445 million breaches identified (Kaspersky, 2021). Furthermore, according to research conducted by the International Telecommunication Union (ITU) in 2020, half of all Internet users have compromised their security.

These breaches are costly. According to the International Business Machine Cooperation (IBM, 2021), the cost of a data breach in an organisation is projected to be $3.92 million US dollars, with an average data breach of 25,575 records every year. Moreover, the study by Williams (2021) reports that, on average, 61 organisations were successfully attacked every week in 2021. Consequently, the study by IBM reports that the world succumbed to a loss of 4.24 billion US dollars in 2021 alone. (International Business Machine Cooperation (IBM), 2021).

There are different factors which affect information system security worldwide. The study by Alotaibi, Furnell and Clarke (2016) reported human factors such as perception, technology democracy, cultural factors, gender, satisfaction, and habits affect information system security. In addition, the study by Assefa and Tensaye (2021) identified technical factors such as awareness and training, accountability, and audit and monitoring. Thus, administrative elements do affect the security profile of the organisation. Such administrative elements include the cyber security policy (Ofori, Anyigba, Ampong, Omoregie & Nyamadi, 2020). Failure to follow ICT rules has a detrimental impact on the security of information systems. Alhogail (2015) found that one of the causes of internet vulnerability is a lack of commitment to the security culture. As a result, issues such as a lack of management support, an inadequate information security policy, and a lack of information security education programmes lead to poor security in corporate information systems (Alhogail, Mirza, & Bakry, 2015; Arbanas & Hrustek, 2019).

It is unarguable that the Information Security Policy is among the critical administrative tools for ensuring data or information security and associated infrastructure. First, the policy formulation process identifies all potential security risks and threats to the organisation (Flowerday & Tuyikeze, 2016). In addition, the IS security policy document development process puts control measures necessary to address weaknesses in risk areas (Alotaibi, Furnell, & Clarke, 2016; Alqahtani, 2017). ColThecument provides a comprehensive guide for the organisation to ensure the security of its information systems assets. Nonetheless, not all security policies are comprehensive enough to guide their users. This position is supported by Lubua and Pretorius (2019), who said that security policies need to be revisited to meet emerging requirements.

Hence, the interest of this study is to evaluate the quality of information system security policies associated with higher learning institutions to address security challenges. The evaluation uses the framework established by ISO/IEC 27000:2018 (2018), Qureshi (2011), Lubua and Pretorius (2019), and Zhaq (2022). The evaluation selected these frameworks because reputable organisations endorse them and specialise in information security policies. The study developed an information system security policy evaluation framework consisting of the following key elements; password

management, email use principles, disaster handling and recovery, hardware and software management, and information handling.

Literature Review

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

Information Systems Security

Evidence shows that human activities are increasingly dependent on information systems. Human beings need information systems for operations and decision-making. The need for a good information system to meet customer satisfaction has increased the use of computers and computer systems (Almazán, Tovar, & Quintero, 2017). In Tanzania, for example, 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%, while 60% of people are subscribers worldwide (International Telecommunication Union, 2021). With this increase, it is indisputable that efficiency in the use requires reliable information systems to enhance the performance of the user organisation (Almazán, Tovar, & Quintero, 2017).

The reliability of information systems is possible if supporting infrastructure and associated resources are safe (Semlambo, Almasi, Liechuka., 2022; Alotaibi, Furnell, & Clarke, 2016; Semlambo, Leichuka & Almasi, 2022). Nevertheless, several factors affect the required level of online safety, as Alotaibi, Furnell and Clarke (2016) and Assefa and Tensaye (2021) reported. Such factors include human-related factors, technical factors, and administrative factors. According to Williams (2021), there is an increase in information systems threats released online daily. Some of these threats include phishing, social engineering, supply chain attacks, zero-day and polymorphic attacks, and IoT and infrastructure attacks (Broadhurst, Skinner, Sifniotis, Matamoros-Macias, & Ipsen, 2018; Lohani, 2019).

To address these threats, the organisation must have a strong administrative foundation, provided through policies governing the use of ICT (Alqahtan, 2017; ISO/IEC 27000:2018, 2018). For this reason, the current study evaluates the quality of information security policies among higher learning institutions.

The Quality of Information Security Policies

The quality policy takes into account technological concerns arising due to new developments in the industry (Lange, Solms, & Gerber, 2015). Ultimately, the policy must enable the organisation to achieve its established security objectives (Siponen, Mahmood, & Pahnila, 2014). The study by Lubua and Pretorius (2019) identified eight quality areas of an Information Security policy. The policy must address data security issues and internet and network services governance concerns and guide the use of company-owned devices. Other quality areas include 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 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.

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 Tanzanian higher 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
	An extended use of default passwords
Email use principles	Attachments management
	Dealing with forwarded emails
	IT 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 2022

Research Methodology

The study used the document analysis approach to examine the quality of information systems security policies in addressing security challenges. The study used selected public higher learning institutions in Tanzania as the case study. 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 (O'Leary, 2014).

Cases for Study

The study focused on public higher learning institutions in Tanzania providing bachelor's degrees and above. These institutions were selected based on their similarities in terms of ownership and sharing of common public ICT infrastructure under the same Internet Service Provider (ISP).

Table 2: Cases for Study

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

Source: Researchers 2022

Data Collection

The data collection process involved eight public higher learning institutions in Tanzania. Private learning institutions were excluded because they were not obliged to use the same Internet Service Provider.

The data collection involved gathering ICT security-related policy documents from all eight selected public higher learning institutions. Data collection followed the security policy focus area and related sub-areas established in Table 1, including password management with sub-areas such as locking workstations while idle, password privacy, password strength, and extended use of default passwords. The focus area is email use principles, including sub-areas like attachment management, dealing with forwarded emails, IT department level of responsibility in email use, managing access to external emails, guidelines on acceptable use of the internet, managing social media use, and guidelines on how to manage the use of own devices for official purposes. The third focus area is disaster handling and recovery, including guidelines on offsite back-ups and managing disasters. The fourth focus area is hardware and software management, which includes guidelines for updating system software and hardware, managing software installations and guidelines on administrative issues. The last focus area is information handling, which includes guidelines on data ownership, information security and classification, and how to dispose of data and information.

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 in Table 1 were studied for each policy to see whether they are well covered. The study shows the similarity and differences in

how such sub-areas are covered for each aspect. Therefore, the study is descriptive, as Edga & Manz (2017) supported.

Findings and Analysis.

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

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 3: Evaluation of Password Management

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

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 4 Evaluation of Email Use Principles

Variable	Compliance Issues		No. of Non-compliance Issues		Total	
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.
Attachments management	2	25	6	75	8	100
Dealing with forwarded emails	1	12.5	7	87.5	8	100
IT department’s level of responsibility in email management	6	75	2	25	8	100
Managing access to external websites	1	12.5	7	87.5	8	100
Guidelines on acceptable use of the internet	5	62.5	3	37.5	8	100
Managing social media use	1	12.5	7	87.5	8	100
Guidelines on how to use own devices for official purposes	1	12.5	7	87.5	8	100

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.

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 5 Evaluation of Disaster Handling And Recovery

Variable	Compliance Issue		No. of Non-compliance Issues		Total	
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.
Guidelines on offsite backup	2	25	6	75	8	100
Guideline on how to manage disasters	1	12.5	7	87.5	8	75

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.

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 6 Evaluation of Hardware and Software Management

Variable	Compliance Issue		No. of Non-compliance Issues		Total	
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.
Software licence management	5	62.5	3	37.5	8	100
Guidelines for upgrading system software and Hardware	5	62.5	3	37.5	8	100
Managing software installation	5	62.5	3	37.5	8	100
Guidelines on administrative issues	5	62.5	3	37.5	8	100

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.

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 7 Evaluation of Information Handling

Variable	Compliance Issue		No. of Non-compliance Issues		Total	
	Freq.	Perc.	Freq.	Perc.	Freq.	Perc.
Guidance on data ownership	4	50	4	50	8	100
Guidance on Information sensitivity and classification	1	12.5	7	75	8	100
Guidance on how to dispose of data and information	1	12.5	7	75	8	100

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.

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. Discussion of each of these elements is presented in the next part

Password Management

As presented in the findings and analysis, this category is divided into four subcategories, starting with locking the workstation while idle. Several locking mechanisms can be used to lock a workstation or lock the screen of a workstation, including passwords (PIN), biometric scanners such as face recognition or fingerprint scanner or voice recognition, virtual keys, temporal keys or remote access, and others such as explained by Alghamdi (2020). As presented in Table 4, 7 out of 8 information system security policies of institutions selected for this study do not compile to this subcategory. This leaves these institutions vulnerable to different information system security threats from anyone who can use these unattended workstations maliciously.

In the subcategory of privacy in password use, as presented in Table 4, findings show that 6 out 8 information system security policies from the selected institutions for this study do not compile to this subcategory. When a password becomes known more than to its intended person, the risk of information confidentiality becomes great, and an unauthorised person can use that login credentials to access restricted or protected information of the institution. For example, Yldrm and Mackie (2019) and Charoen (2014) discussed using software to analyse the strength of passwords. They also stressed the importance of password memorability to avoid writing it down on a piece of paper that unauthorised individuals can find and use as a security breach while all fault falls on the owner of the password,

Also, Password strength emphasised by researchers includes but is not limited to the use of a 'password strength meter', which tells whether the chosen password is 'weak', 'strong' or 'very strong' based on the length of the password (M. Yıldırım & I. Mackie, 2019). Passwords created using a password strength metre have been found to be more secure than normal passwords, thus providing better security to an organisation's information systems, as Simon and Cheung (2014) strongly concur. The need for ICT users to have reliable and secure passwords in a learning environment keeps increasing for different security reasons (IAU, 2020). Unfortunately, this subcategory has not been found in any of the information system security policies from all the 8 institutions selected for this study. Thus, public higher learning institutions in Tanzania information system security policies need to emphasise the strength of passwords to avoid security threats from using weak and obvious passwords such as person names and date of birth.

Using default passwords over an extended period is another subcategory that was not found in the case institutions' information systems security policies. Numerous programmes permit user names and passwords to contain only one character. The user may opt for a more complex password. Still, as special characters and total character counts are frequently unnecessary, the user may opt for the simplest, most practical credential option (Knierem, Zhang, Levine, Breitinger, & Baggili, 2018). 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.

Email Use Principles

The first subcategory in Email use principles was attachment management, as shown in Table 5 with 6 non-compliant levels out of 8 information systems security policies reviewed from case institutions. It is important to have restrictions on the size of emails and attachments that can be shared via emails, 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).

Dealing with forwarded emails was the second subcategory with 7 non-compliant levels out of 8 information systems security policies reviewed from the case institutions. Forwarded email can be used as a source attack in an organisation's information system if improperly managed. They can be a result of phishing attacks as explained by Broadhurst, Skinner, Sifniotis, Matamoros-Macias and Ipsen (2018), Chaudhry, Chaudhry and Rittenhouse (2016), and Gupta, Arachchilage and Psannis,, (2018).

IT Department's Level of Responsibility in Email Management was another subcategory with 2 non-compliant levels out of 8 information systems security policies from case institutions. The level of email management captured by these two institutions complies with those of other researchers like Broadhurst, Skinner, Sifniotis, Matamoros-Macias and Ipsen (2018), Chaudhry, Chaudhry and Rittenhouse (2016), and Gupta, Arachchilage and Psannis (2018). These are the same policies developed in 2012 and renewed in 2017; the others were developed in 2018 and renewed in 2022. Appropriate email management by the IT department through well-developed policies helps reduce information system security incidences in learning institutions.

Managing access to external websites had 7 non-compliant levels out of 8 information systems security policies selected from case institutions. To maintain proper information system security in institutions, clear management of accessing external websites needs to be captured by information system security policy. This is because these websites can be used to gain access to the institution's system through phishing attacks, social engineering attacks, or viruses and ransomware (Chaudhry, Chaudhry, & Rittenhouse, 2016; Gupta, Arachchilage, & Psannis, 2018).

Guideline on acceptable internet use was reflected to 5 of the information system security policies from case institutions. However, the remaining 3 information system security policies from the case institutions had poor compliance levels in this subcategory. The amount of data a person can access in a day via an institution's internet, the types of services that can be accessed within and restrictions on what cannot be accessed while using private internet, such as internet coffee, restrictions on what can be sent and received via institution internet, restriction on content that can be broadcasted on institution internet and restrictions on devices that can be used to access institution internet. Other researchers, such as Apuke and Iyendo (2018), also cover these acceptable uses of the Internet.

Policies of public higher learning institutions should contain enough guidelines on safe and acceptable usage of the institution's internet to avoid information system security incidences.

Findings showed that managing social media users had a poor compliment level resulting from different information system security threats and vulnerabilities from using social media in learning institutions' networks. For example, Mitra and Gilbert (2012) discussed the impact of using social media to discuss office-related issues and gossip and how they can affect productivity and the security of an organisation's information system. Also, Väyrynen, Hekkala and Wiander (2012) pointed out the effects of social media on employees and organisations, including malware, spam, scams, phishing, identity theft, and information leakage (intentional or unintentional), reputation risk, and control of reputation. In contrast, Majid and Kouser (2019) listed the causes of risk in social media, including 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.
Regardless of the advantages social networking sites can bring to the table for both students and facilitators in learning environments (Lubua, Semlambo, & Pritorius, 2017), They are not without their challenges. If not managed properly, social networking sites can harm productivity in the workplace based on time spent on social networking sites instead of performing an organisation's core objectives, as explained by Awolusi (2012). Without appropriate considerations of adequate controls of the use of social networking sites through information system security policies, it will result in challenges such as wastage of time, low productivity, lower job concentration, circulating wrong information, lack of confidentiality, and misunderstanding at work, as explained by Eliringia (2017). Public higher learning institutions need information system security policies that adequately address the appropriate use of social networking sites and restrictions on some of the social networking sites that can damage an organisation's core objectives.

Guideline on how to use own devices for office purposes had a poor compliant level of 7 non-compliant information system security policies out of 8 selected from the case institutions. This study found that this issue was not covered in any of the policies chosen for the case study (Sánchez, López-Belmonte, Moreno-Guerrero, Reche, & Cabrera, 2020). This increases the chances of information system security vulnerabilities, as elaborated by other researchers such as Tinmaz and Lee (2019) and Retnowardhani, Diputra, and Triana (2019).

In supporting online learning, the institution's ICT policies must evaluate various processes and procedures such as online assessment and examination systems, mobile learning technologies, and the installation of video conferencing facilities (Semlambo, Almasi, Liechuka., 2022; Semlambo, Leichuka & Almasi, 2022). Some institutions' ICT policies have completely left out mobile computing aspects. As potential as mobile facilities are in today's learning environments, higher learning institutions' ICT policies need to specify safe measures taken to protect users and the institute from potential threats that come with connecting personal hardwires (mobile phones, tablets, and laptops) with the institution's network, such as Bring Your Own Device (BYOD) restrictions. A few policies have BYOD restrictions explained, while other institutions have completely left it out of their policies. Allowing users to bring their own devices and connect to the institution's network brings many risks, as most employee devices come with malware due to access to suspicious websites and software (Jahanbakhsh, Amini-Rarani, Tahmasebian, & Shahbazi, 2020). ICT/ Information System security policies of public higher learning institutions need to provide straight and detailed information on how users can protect themselves from such vulnerabilities.

Disaster Handling and Recovery

Assessing the effectiveness of information system security policies, as outlined in Table 1, involves considering disaster management and recovery. Key factors in this evaluation encompass recommendations for offsite data backups and protocols for handling unforeseen catastrophic events.

Guidelines on offsite backup was one of the subcategories in this category with 6 non-compliant levels out of 8 information systems security policies evaluated from the case institutions. 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), concur. This study found minimal attention has been given to the importance of regular offsite backup to save data from different kinds of disasters that may occur in the institution, as explained in the next sub-category.

Guidelines on managing disaster had 7 non-compliant kevels out of 8 information system security policies from the case institutions. Some of the policies in public higher learning institutions in Tanzania have completely left this part out with no clarification or justification on how any kind of disaster to ICT infrastructure can be handled. Information System security policies should clearly state how disasters caused by natural occurrences or by humans can be handled and their specific procedures for dealing with the situation (Hina & Dominic, 2018). 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).

Hardware and Software Management

Evaluating the effectiveness of information system security policies, as outlined in Table 1, involves examining hardware and software management. This key aspect encompasses various categories such as software license management, protocols for updating system software and hardware, overseeing software installation, and guidelines for addressing administrative issues.

In the subcategory of software license management, 3 non-compliant out of 8 information systems security policies were reviewed from the case institutions. Software licence issue needs proper notes on institutions' policies as software can be used to penetrate an organisation's infrastructure and compromise information system security. (Yang, Hosseinian-Far, Jraisat, & Rangaswamy, 2021).

The guideline for updating system software and hardware also had a non-compliant level of 3 out of 8 information system security policies reviewed by the case institutions. Other researchers emphasised issues like user requirements and feedback, user recommendations, guidelines on yearly maintenance, system architecture and design schemes in platforms with new hardware, storage and indexing techniques in platforms with new hardware, query processing and optimisation in platforms with new hardware, and transaction processing in platforms with new hardware (Wei Pan, Zhang, & Weng, 2018).

This study found that most public higher education policies do not have appropriate guidance on hardware usage, resulting in institutions using outdated hardware, such as PENTIUM computers, which are incompatible with most of today's software. Most institutions' use policies have no guidance on appropriate government guidelines on ICT infrastructure usage, such as the use of ICT hardware for more than ten (10) years, which is against government procurement regulations that hardware

should not be used for more than 10 years (The Public Procurement Act (410), 2013). Information System security policies of public higher learning institutions should clearly state hardware and software management for appropriate use of ICT infrastructures and emphasise appropriate training and awareness programmes before introducing new hardware or software.

In managing software installation, to maintain institutional information system security, institution policies need to have a clear and well-defined note on who will be responsible for software installation, when and where, brands of software, use of open source software and other software installation restrictions as explained by Yang, Hosseinian-Far, Jraisat, and Rangaswamy (2021).).

Guideline in administrative issues, the study discovered that, due to centralised working culture and different organisational structures, managers are frequently excluded from committees involved in the formulation of Information System security policies (United Nations, 2016). In most cases in Tanzania's public higher learning institutions, even the IT main office had no main ownership of the information system security policy apart from the selected few that formulate it in the ICT policy committee. This study's findings revealed that employees' involvement in creating institutions' ICT and information system security policies is very poor. Thus, these policies are being created only for compliance by the few that formulate the policy creation committee, and afterwards, these policies are not shared with all employees. Instead, these policies are treated as very confidential documents that even employees of that organisation cannot access; hence leads to the question of whom these policies were created for.

These claims are supported by other researchers, such as Hina and Dominic (2018). To have a clear understanding of all potential security areas of the organisation, all employees of that organisation need to be involved in the policy creation process (Alqahtan, 2017). The success of any organisation's information system security policyepends highly on employee behaviour and involvement in policy creation (Glaspie & Karwowski, 2018). The involvement of employees in information system security policies will motivate security habits and help eliminate security risk behaviours such as sharing log-in credentials (Astakhova, 2016; Robinson, 2019).

The study found the use of informal guidelines in place of policies. These institutions mostly use this relaxed way as an intervention of the IT department to safeguard institutions against information system security threats. This intervention using informal guidelines has been observed to delay the approval of formal Information System security policies from the top management (Korhonen, Hiekkanen, & Mykkänen, 2012). Because many information system security policies of public higher learning institutions in Tanzania require additional informal guidelines, it is evident that they are inadequate against information security challenges. This is because stakeholders aren't involved enough, and we depend too much on them, making information system security incidents more likely (Gagliardi, Hankin, Gal-Ezer, McGettrick, & Meitern, 2016). As some ICT policy documents have indicated, all employees should have regular training and awareness programmes about information system security policies. However, they have no application as the policies remain in documents stored somewhere just for compliance, as supported by other researchers such as Hina and Dominic (2018).

Information Handling

Assessing the effectiveness of information system security policies, as established in Table 1, involves considering the handling of information. This variable is crucial and encompasses various categories, including guidelines on data ownership, information sensitivity and classification

guidance, and instructions on proper data and information disposal. The evaluation results are summarised in Table 8.

Guidance on data ownership was the first subcategory in this category; it had 4 non-compliant levels out of 8 information system security policies reviewed by the case institutions. 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.

Guidance on information sensitivity and classification had 7 non-compliant out of 8 information systems security policies reviewed from the case institutions. Information system security policies must ensure that the management of public higher learning institutions prioritises information system security. This is due to its sensitive nature and the use of ICT facilities to achieve organisational objectives daily. 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).

Guidance on how to dispose of data and information was the last subcategory in this category with 7 non-compliant levels out of 8 information systems security policies reviewed from the case institutions. It's normal for employees from all departments (management and other supporting staff) to clean their offices regularly and dispose of office-related documents as they see fit, disregarding the information system security threats they can bring to themselves and their institutions. Data disposal methods to be considered in the institution should centre on data anonymisation, deletion, crypto shredding, degaussing, and destruction. (Kablawi, 2022).

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 these findings, the study had the following recommendations; regular awareness and training programmes must be conducted for all employees of public higher learning institutions in Tanzania about managing their passwords. The same applies to the management of emails, such as attachment management, dealing with forwarded emails, IT department level of responsibilities in email management, managing access to external websites, guidelines on acceptable use of the internet, managing social media use and guidelines on how to use one device for office purposes. Also, the management of public higher learning institutions should have strong guidelines on managing disasters from natural to human-based, including backups. In hardware and software management, the study recommends that improvements include step-by-step guidelines on software updating so that technicians and users can understand guidelines. And lastly, training and awareness programs should be considered for all public higher learning institutions employees regarding data ownership, information sensitivity and classification and how to dispose of data and information.

This study recommends using a harmonised, standardised, well-developed information system security policy framework for all public higher learning institutions in Tanzania. This could help in centralising information system security threats. Documenting and allowing these institutions to learn from each other's experiences with information system security threats will help ensure they are under control and will not strike again. Also, the study proposed the following to the government;

- Governments and policymakers must appoint a dependable agency to ensure that no public higher learning institution operates without an ICT and information systems security policy.
- Perform field visitations to these institutions to ensure regular awareness and training programmes are performed at least twice a year.
- Government agencies should review these policies at least every four (4) years to accommodate new technological changes whenever necessary. This will also help information system security policies remain current and proactive against all security threats and vulnerabilities.
- The agency needs to ensure that developed policies can adequately address information system security challenges facing public higher learning institutions.

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 Organisational 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. j*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 Secretariat - Mara Region.* Morogoro: Mzumbe University.

Fadler, M., & Legner, C. (2022). Data Ownership Revisited: Clarifying 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 Science, 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 Worldwide Resources for Higher Education Institutions.* International Association of Universities.

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

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

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 Techniques.* 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 on 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. *Sustainability, 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 Backup 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. E*uropean Conference on Information Systems (ECIS)* (pp. 1-13). Barcelona, Spain: European 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.