6th International Academic Conference on MANAGEMENT and ECONOMICS

24 - 26 March, 2023
Oxford, The United Kingdom

Assessing the Conformity to ISO27001 Security Policy of Information Systems Policies of Universities in the SADC Region

Oduronke T. Eyitayo[1], Ontiretse Ishmael[2]
[1]School of Computing and Creative Technology
University of the West of England, United Kingdom.
[2] Department of Computer Science and Applied physics,
Atlantic Technological University, Ireland

Abstract

It is very important for universities to devise strategies for realising their mandate and one of those strategies is to leverage on information systems for improved service efficiency and realising business goals. This is bearing in mind that organisational strategies determine which information systems to implement, and which policies guide the use of the Information Systems. Universities these days rely heavily on ICT resources for the core teaching and research activities. The need for clear IS policies and procedures are therefore needed for universities to be successful in their mandate. A lot of universities these days spend time and resources creating their business processes, strategies and policies and passing it through their different structures for approval. However, there is no clear evidence that the policies are visible to the intended audience. This paper therefore investigates the online visibility of IS policies of Southern African public universities in 15 countries in Southern African Development Community (SADC). Region and the conformity to ISO27001 standards of the IS policies. These universities are selected from those with membership of the Southern African Regional Universities Association (SARUA).

Keywords: IS Policies; ISO27001 Security Policy; SADC; Visibilities

1. Introduction

Information Systems (IS) have gained popularity as a key resource in driving business strategies and obtaining operational excellence. Information technology on the other hand is a subset of information systems (Checkland & Holwell, 1998). In this paper, we look at IS policies as comprising of policies on people, processes, and technologies. This means it will include both IT (Information Technology) strategies and Information Security Strategies. Policies are high-level statements, which ensure or guide compliance. In relation to Information System (IS) strategy, policy ensures compliance to strategy. They address pertinent issues, such as what constitutes acceptable behaviour by the users. IS policies as comprising of policies on people, processes, and technologies (Bansal et al., 2020). This means it will include both IT (Information Technology) strategies and Information Security Strategies. More universities these days are relying heavily on ICT resources for the core teaching and research activities. The need for clear IS policies and procedures are therefore needed for universities to be successful in their mandate. However, it seems that most developing countries lag behind in the appropriate use of technology (Macbean & Snowden, 2021). Proper procedures are sometimes ignored, and this seems to be the case as well in universities and other institutions of higher learning. The critical role played by these IS policy in overall development issues appears to have been neglected in the pursuit of the use of IS. Policy documents should therefore establish the mechanism for an organisation to proactively manage information security.

One of the most significant role of information security policy is to precisely specify user's rights and responsibilities and to successfully communicate it to all users, to ensure there is a mutual and coherent understanding of information security that is embraced by the organisation.(Ghazvini et al., 2018). The goal is providing access to only those authorised personnel who need the access, keeping the information accurate and complete and making sure the information is available to the authorised user when they need it. There are different categories of IS Policies such as Information security policy, acceptable use policy, web policy, data management policy, digital copyright compliance, IT standards, IT accessibility, acceptable right policy, Bring your own device policy, social media policy, Incident response policy and procedures, and others (GRIT Realters, 2018). Which of these policies are essential for the universities? What should the policies contain for universities?

The main purpose of this study is to assess the visibility of IS policies and conformity to ISO27001 Security Policy of Information Systems (IS) Policies of Universities in the SADC region.

This then leads the following objectives:

- To investigate the visibility of IS policies of public universities in SADC region.

- To critically analyse the overall structure of the policies of the universities.
- To assess the conformity with the ISO27001 standard.
- To identify the more critical policies for the African setup.

2. IS Policies and Universities

Information Security policies in Universities around the world have developed over the years (Doherty et al., 2009). Many universities have their policies visible online. Even though there has been a lot of visibility of IS policies in the developed world, less visibility of the IS policies has been a source of concern in developing countries. (Higgins, 1999) said, "Without a policy, security practices will be developed without clear demarcation of objectives and responsibilities". This is also supported by (Doherty et al., 2009) who stated that the primary objective of information security policy is to define the users' rights and responsibilities in terms of information within an organisation. (Doherty et al., 2009) also emphasise that effective information security policies assist users to understand what acceptable and responsible behaviour in information resources is and will assist in establishing a safe information environment.

Many organisations such as universities have put in place information Systems Management (ISM)(Bright & Asare, 2019; Everett, 2011). Compliance levels have been found to increase in organisations that were more aware of their ISM issues, which could lead to improved information security policy and business continuity plans within their organizations.(Järveläinen, 2012). The ISO 27001 standard provides guidance to a sound information security management system (ISMS)(Hsu et al., 2016). This standard puts technology, process and people in place (Shojaie et al., 2015). The ISO 27001 information security management system standard is well respected and internationally recognised (Everett, 2011). Implementing Information Security Management System (ISMS) can help to identify, manage and reduce any information security threats in the data centre. One of widely accepted ISMS standard today is ISO 27001. Existing standards such as ISO 27001 are designed to provide general information security that can be applied to different environments (Achmadi et al., 2018) .

3. Methodology

The study focuses on the Information System, Information Security or IT policies. This was done by studying websites of universities to establish visibility. The Universities chosen were members of the Southern African using SARUA Universities. The study uses critical analysis methodology. In evaluation, the study uses the ISO27001 Security Policy.

Critical analysis methodology uses a three-step approach in studying the policies of SADC universities. The first is contextualising the problem by studying the websites, the second is analysing the websites to explore the situation and lastly evaluating the results

Fifteen (15) SADC countries were studied. Public Universities belonging to SARUA were identified. Fifty-two (52) Universities were English speaking. Seventeen (17) universities, which are non-English speaking, were excluded. Twenty (20) universities from SADC have visibility online. Visibility is about 38.5% overall of which 23% (60 % of the total) was from South Africa alone. Four (4) other Southern African Universities (Malawi, Seychelles, Tanzania and Zimbabwe) shared the remaining 40 % visibility. Table 1 gives details of the number of public universities found on SARUA website, Languages used and the IS policy visibility in these universities (*Sarua*, 2019).

Table 1: IS policy visibility of universities found on the SARUA website

Country	SARUA Universities	Languages	IS Policy Visibility
Angola (Not in SARUA)	0	Portuguese	Web site content not in English
Botswana	2	English	0
Comoros (Not in SARUA)	0	English	0
Democratic Republic of Congo (DRC)	5	French / English	Web site content not in English
Lesotho	1	English	0
Madagascar	6	French/ English	Web site content not in English
Malawi	2	English	1
Mauritius	2	French/ English	1 (Intranet only)
Mozambique	4	Portuguese/ English	Web site content not in English
Namibia	1	English	0
Seychelles	1	French/English	1
South Africa	23	English	13 (1 not assessible)
Eswatini	1	English	0
Tanzania	9	English	4
Zambia	3	English	0
Zimbabwe	9	English	2

In answering the question, “What should the content of policies for Universities?” The study uses ISO27001 Policy Standard to evaluate coverage. Ten areas related Information Security Policy were selected. The basic elements are shown in Table 2. (*Sarua*, 2021)

Table 1 : Related ISO27001 Policy Standard.

	Code	IS Policy related Standard	Areas covered
1	ISP	Information Security and Policy	Information Security policy
2	CAIS	Controlling Access to Information and Systems	Managing User Access; Managing User Access; Managing User Access
3	PID	Processing Information and Documents	Network Security; E-mail and the Worldwide Web; Backup, Recovery and Archiving; Document Handling; Securing Data
4	SHP	Securing Hardware, Peripherals and Other Equipment	Working Off Premises or Using Outsourced Processing
5	CCC	Combating Cyber Crime	Combating Cyber Crime
6	DPC	Dealing with Premises Related Considerations	Premises Security; Data Stores
7	API	Addressing Personnel Issues Relating to Security	Personnel Information Security Responsibilities
8	DTA	Delivering Training and Staff Awareness	Awareness; Training
9	CLR	Complying With Legal and Policy Requirements	Complying with Information Security Policy
10	DRI	Detecting And Responding to Is Incidents	Reporting Information Security Incidents; Corrective Activity

4. Results and Analysis

Different countries were analysed using the identified universities from SARUA, policies and policy coverage, as well as their last reviewed date.

Malawi

There is only one Public University in Malawi with a visible IS policy. Mzuzu University has Social media policy, ICT security policy, Network ICT User agreement and ICT breach policy of which the last received for the policy is not stated. The details are shown in Table 3.(Mzuzu, 2020)

Table 3: Visible IS Policies at University in Malawi

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
Malawi	Mzuzu University	Social media policy	Personal and professional reputations in social media participation.	Not Stated
		ICT security policy	Computer system availability, Conservation and efficient use of ICT resources, Integrity and confidentiality of university data and information	
		Network ICT User agreement	Electronic Mail and Network Security	
		ICT breach policy	Management of breaches, Breach Reporting, Internet breach, Breach penalties	

Seychelles

University of Seychelles is the only public university with IT services and Guidelines policy visible. The details are shown in Table 4 (Seychelles University, 2021).

Table 4: Visible IS Policy at University in Seychelles

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
Seychelles	University of Seychelles	IT services and Guidelines	Important device security information and the use of electronic communications	Not Stated

South Africa

South Africa has several public universities in SARUA that have their policies visible online. They are: University of Pretoria, University of Cape Town, University of Fort Hare, University of the Free State, University of KwaZulu Natal, University of Stellenbosch, University of the Western Cape and University of the Witwatersrand. Some were studied. The details of the universities/policies covered are shown in Tables 5 to 9.

University of Pretoria has Policy on Acceptable Use of Computing Resources, Electronic Communications Policy, Information Security Policy, Malware Prevention Policy, Network Security Policy, Password Policy, Portable Hardware and Removable Media Policy and Wireless Network Policy use. The details are shown in Table 5.

Table5: Visible IS Policies at the University of Pretoria

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
South Africa	University of Pretoria	Policy on Acceptable Use of Computing Resources	Guide on how to use all University resources	2014-02-18
		Electronic Communications Policy	Securing and maintaining computer network, equipment and communication facilities	2017/02/15
		Information Security Policy	Identifying the rules for accessing, using, maintaining, administrating and managing the University's IT assets and resource	2019-06-24 .
		Malware Prevention Policy	Defining the responsibilities of users to prevent network virus outbreaks and other types of malware attacks	Draft 2012-08-28
		Network Security Policy	Access to the institution's networks and the information carried on them will be protected at all times	2017-11-17
		Password Policy	Services and users responsibilities regarding the management and use of passwords to prevent unauthorised access, and compromise or theft of information.	2017-02-15.
		Portable Hardware and Removable Media Policy	To protect the integrity and security of the private and confidential Institutional information	2017-02-03
		Wireless Network Policy	Standards and procedures to regulate the provisioning and secure use of the wireless data network	

University of Cape Town has several visible policies and guidelines: Internet and email policy, UCT network, Anti-virus, Passwords, Hardware and software, Student labs, Metadata and Web publishing. The details are shown in Table 6.

University of KwaZulu Natal have the following visible policies: Internet Facilities, Access, Acceptable Use, Misuse, Rights and Responsibilities, Confidentiality, Passwords, Penalties, Resource Limits and User Responsibility.

The University of Stellenbosch has the following visible policies: Electronic Communication Policy, Electronic Identity Validation Regulation, IT End User and Media Regulation Identity and Access Management Policy, Information, Security Regulations, Interim Access Regulation, internet Access as well as Password Regulations and Records Management Policy. Details are shown in Table 7.

Table 6: Visible IS Policies at University of Cape Town

	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
South Africa	University of Cape Town	Internet and email policy	Policy and rules on Internet and email use ; Take-down procedure; ISPA Code of Conduct	1 June 2016
			The email naming standard	May 2013
			The email nickname naming standard	25 Feb 2011
			Retention of old non-uct@ac.za email addresses	Nov 2010
		UCT network	The UCT network as a core service	31 July 2019
			UCT's network peering policy	January 2008
			UCT Perimeter; Firewall Policy	31 July 2019
			Acceptable use of Guest Wireless Access	
		Anti-virus	Policy on prevention of infection of computer networks and technology systems from computer viruses and other malicious code	25 July 2014
		Passwords	Policy on passwords	19 Novr 2015
			Appropriate use of computer facilities policy	4 May 2011
		Hardware and software	ICTS policy on moving computer equipment	1 January 2015
			Policy on Disposal / Internal transfer of UCT IT Equipment	25 Feb 2011
			Policy on unsecured computers at UCT	July 2016
			Supported hardware policy	4 May 2011
			Exceptions to the supported hardware policy	
			Software support policy	28 Feb 2012
		Student labs	Roles, responsibilities, rules and regulations of student computing labs	17 Nov 2011
		Metadata	Managing metadata and it's application to information assets and services	26 May 2011
		Web publishing	Web Content Management Policy	
			Web Hosting Policy	25 January 2013
		Guidelines	Domain Name Policy; Network access from residences	
			Communications; Structured Cabling System guidelines and specifications for external contractors; A guide to writing effective email messages	

Table 8: Visible IS Policy at University of the Western Cape

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
South Africa	University of the Western Cape	UWC policy ICT	ICT information security policy, Internet and Email Usage, Access Control, Security, Awareness and Training; Security Incident Management, Networks, Firewalls, Encryption, Remote Access, Anti-Malware, Physical and Environmental Security	2004/5

Table 7: Visible IS Polices at University of Stellenbosch

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
South Africa	University of Stellenbosch	Electronic Communication Policy	Framework for the use of the electronic communication facilities	2003/12/01 -
		Electronic Identity Validation Regulation	Ensuring people's identity is validated before an electronic identity is created	2012/12/13
		IT End User and Media Regulation Identity and Access Management Policy	Establishing rules for the appropriate use of end-user equipment and media.	2015/06/01
		Information, Security Regulations, Interim Access Regulation	Ensure that the University information system assets are used for the purposes which they were intended	2010/10/13
		Internet Access	Guidelines for access to the Internet	2009/05/04
		Password Regulations	Standards and guidelines for the creation and protection of passwords	2008/06/09 -
		Records Management Policy	Handling records in accordance with fiscal, legal and historical requirements	2016/11/28

University of Western Cape has a visible policy on ICT that covers several aspects. Details are shown in Table 8.

University of Witwatersrand has visible policy on Information Communication Technology (ICT) systems and services. Details are shown in Table 9.

Table 9: Visible IS Policy at University of Witwatersrand

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
South Africa	University of the Witwatersrand	Information Communication Technology (ICT) systems and services	General Use and Ownership; Security and Proprietary Information; Unacceptable Use System and Network Activities; Email and Communications Activities and Enforcement.	

Tanzania

Tanzania has four public Universities with visible IS policies. They are: Muhimbili University of Health and Allied Sciences, Sokoine University of Agriculture, University of Dar-es-salaam and University of Dodoma.

The Muhimbili University of Health And Allied Sciences has the following visible policies: ICT Security Governance and Management, Security of ICT Assets and Access Control and Management. Details are shown in Table 10.

Table 10: Visible IS Policies at Muhimbili University of Health and Allied Sciences

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
Tanzania	Muhimbili University of Health And Allied Sciences	ICT Security Governance and Management	ICT security practices	1st November 2017.
		Security of ICT Assets	ICT assets protection and access control	
		Access Control and Management	Ensure that access to University ICT	

Sokoine University of Agriculture has a visible policy on ICT Infrastructure and Services. Details are shown in Table 11.

Table 11: Visible IS Policy at Sokoine University of Agriculture

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
Tanzania	Sokoine University of Agriculture	ICT Infrastructure and Services	Developing and maintaining efficient and effective LAN	Not stated

University of Dodoma has only the ICT Policy statements visible. Details are shown in Table 12.

Table 12: Visible IS Policy at University of Dodoma

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
Tanzania	University of Dodoma	Dodoma ICT Policy Statements	University Data Communications Network and Services;Cyber Security. Software Development and Acquisition; ICT Services Management , ICT Skills Capacity Building;Telecommunications and Unified Communications.;ICT Procurement, Social Media., Software licensing and ownership. Information Systems and Data Warehousing Special Needs ICT Usage, ICT Infrastructure and Services Maintenance	2018

Zimbabwe

Zimbabwe has only two public Universities with visible IS policies. Lupane State University has the following visible policies: email system, databases, integrated systems, operating systems, internet, telephone systems as well as wireless communication, printers, and copiers. Details are shown in Table 13.

Table 13: Visible IS Policy at Lupane State University

Country	Name of the university	Policy Title	Policy Coverage	Policy last reviewed
Zimbabwe	Lupane State University	Email system, databases, integrated systems, operating systems, internet, telephone systems, wireless communication, printers and copiers.	Email , Computer Viruses , Offensive or obscene e-mail , Confidentiality , ICTS department Emails , Internet , Safeguarding Access to Workstations , Equipment movement / loans , Hardware , Software , Training ICT staff , Computer rooms and ICT hardware usage , ICT Usage , Student's email and Finance	

5. Discussions

Countries that have visible policies include Malawi, Seychelles, South Africa, Tanzania and Zimbabwe. Some of the Universities did not have date last reviewed while Some Universities were reviewed in 2003, which is a source of concern since the rate of growth technology is quite rapid. South Africa Universities seems to be visible and have a lot of the policies detailed Universities used titles suitable for their needs Online contents cover a mixture of policies and guidelines (Procedures). A summary of the findings is shown in Table 14.

Table 14: Summary of findings

	Universities									
		ISP	**CAIS**	**PID**	**SHP**	**CCC**	**DPC**	**API**	**DTA**	**CLR**	**DRI**
1	Mzuzu University	√	√	√	√	x	x	√	x	√	√
2	University of Seychelles	√	√	√	√	x	x	x	x	x	√
3	Kwazulu Natal University	√	√	√	√	√	√	√	**x**	√	√
4	University of Pretoria	√	√	√	√	√	√	√	√	√	√
5	North-West University	√	√	√	√	x	√	√	√	√	√
6	University of Cape Town(UCT)	√	√	√	√	√	√	√	√	√	√
7	University of Stellenbosch	√	√	√	√	√	√	√	x	√	√
8	University of the Western Cape	√	√	√	√	√	√	√	√	√	√
9	University of the Witwatersrand	√	√	√	√	√	√	√	√	√	√
10	University of Dodoma	√	√	√	√	√	√	√	√	√	√
11	Muhimbili Universiy of Health and Allied Sciences	√	√	√	√	x	√	√	√	√	√
12	University of Dar es Salaam	√	√	√	√	x	√	√	√	√	√
13	Lupane State University	√	√	√	√	x	√	√	√	√	√
14	Chinhoyi University of Technology	√	√	√	√	√	√	x	x	√	√
15	Sokoine University of Agriculture	√	√	√	√	x	√	√	√	√	√

Key: **ISP:** Information Security and Policy; **CAIS:** Controlling Access to Information and Systems; **PID:** Processing Information And Documents; **SHP:** Securing Hardware, Peripherals And Other Equipment ; **CCC:** Combating Cyber Crime ; **DPC:** Dealing With Premises Related Considerations and **API:** Addressing Personnel Issues Relating To Security

Out of the 90% of the countries with online visibility, 70% of the components of the ISO27001 that were evaluated were present. Four universities from South Africa and one from Tanzania had all the identified components of the ISO27001 that were evaluated. Most of the missing components were Combating Cyber Crime and Delivering Training and DTA Awareness

Recommendations and conclusion

Many of the Universities (62%) do not have visibility, most of those with visibility do not have Combating Cyber Crime, and Delivering Training and STA Awareness components. Research has shown that lack of communication of policies will in turn affect compliance and become a threat to security. We are therefore recommending that policies should be made visible, communicated and the users made aware of the policies and the act of non-compliance. Information Security must be accessible from the University website. However, deemed to be private to the University should appear on the University Intranet. Policies and procedures are rendered useless if they are neglected and if those who are in charge fail to effectively communicate them to those they are intended for, in this case staff and students. Employee awareness is one of the greatest challenges that organizations must face in order to achieve their required level of security. Information security awareness is important part increasing awareness of security issues, there can be major problems if organizations do not realize the importance information security awareness amongst users. Corporate Citizenship Information Security Awareness and Training Programs is concerned with how employees gain an understanding of appropriate IS culture and practice through awareness raising and training programs. Mitchell, Marcella and Baxter (1999) found that information security awareness was concentrated around the IT department and did not extend to IT users. Information security awareness will therefore provide staff training or development programs to employees.

References

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 149–157. https://doi.org/10.1109/IWBIS.2018.8471700

Bansal, G., Muzatko, S., & Shin, S. (2020). Information system security policy noncompliance: the role of situation-specific ethical orientation. *Information Technology & People*, *ahead-of-p*. https://doi.org/10.1108/ITP-03-2019-0109

Bright, A. A., & Asare, G. (2019). The Impact of Management Information System on University of Education Winneba , Kumasi Campus. *European Journal of Research and Reflection in Management Sciences*, *7*(1), 1–20.

Checkland, P., & Holwell, S. (1998). *Information, Systems and Information Systems: Making Sense of the Field*. Wiley.

Doherty, N., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management*, *29*, 449–457. `https://doi.org/10.1016/j.ijinfomgt.2009.05.003

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud & Security*, *2011*(1), 5–7. https://doi.org/10.1016/S1361-3723(11)70005-7

Ghazvini, A., Shukur, Z., & Hood, Z. (2018). Review of information security policy based on content coverage and online presentation in higher education. *International Journal of Advanced Computer Science and Applications*, *9*(8), 410–423. https://doi.org/10.14569/ijacsa.2018.090853

GRIT Realters. (2018). *Information Security , Communications and Acceptable Use Policy*. *June*, 1–13.

Higgins, H. N. (1999). Corporate system security: towards an integrated management approach. *Inf. Manag. Comput. Secur.*, *7*, 217–222.

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 4842–4848. https://doi.org/10.1109/HICSS.2016.600

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*. https://doi.org/10.1108/09685221211286511

Macbean, A., & Snowden, P. (2021). *The United Nations Conference on Trade Aid and Development (UNCTAD)* (pp. 93–110). https://doi.org/10.4324/9781003226987-5

Mzuzu. (2020). *Mzuzu University*.

Sarua. (2019). Nova/TechNibo, Rustic.

Seychelles University. (2020). *Seychelles | SARUA*.

Shojaie, B., Federrath, H., & Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. *2015 10th International Conference on Availability, Reliability and Security*, 159–167. https://doi.org/10.1109/ARES.2015.25

University of Mauritius. (2020). *University of Mauritius - Home*.