ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

An Evaluation of the Implementation of Information Communication Technology Procedures in Assuring the Information Security Standards in Colleges of Education in Nigeria

Salami Afolabi Kehinde

PhD Student, Department of Information Technology, School of Computing and Information Technology

Kampala International University, Uganda. [1]

ABSTRACT: The study assessed the implementation, enforcement and compliance of Information Communication Technology ([CT) policies in assuring the information security standards in thirteen Colleges of Education whose selection was based on gee political zones of Federal Republic of Nigeria. The study employed cross sectional survey design where the population considered was 1,593 and only took a sample of 118 and data was collected using questionnaires, interviews and documentary reviews. The study found that ICT policy implementation and information security mechanisms were still at basic though in most instances were satisfactorily implemented. Further revealed that the changing nature of knowledge and changing capabilities of technology require colleges of education to implement ICT in their teaching roles to enable the high levels of know-how and develop the skills of ICT innovations in colleges of Education. The majority of users in surveyed had basic security awareness as instituted by institutions' requirements before gaining access to ICT facilities. The study found that there must be constant monitoring of enforcement and compliance put in place. The study also revealed that security risk levels and vulnerabilities are reduced, despite the college ICT facilities, users adhere to the basic institutional security requirements. Finally, in the same light, implementation of ICT policies was found to significantly affect the level of information security. Therefore, it can be concluded that good implementation of ICT policies is a prerequisite for high level performance of information security. The study recommended an in-depth detailed comprehensive implementation of the following ICT policies in order to ensure information security in terms of confidentiality, integrity and availability; access control mechanisms, terms and conditions ofICT usage, backup and recovery mechanism and disaster recovery mechanisms. In addition, regular training of ICT personnel, teaching and non-teaching staff of the colleges and students should be periodically conducted through seminars, workshop and short period professional courses to keep them informed of the technological changes. The Federal Colleges of Education must employ the five pillars of information security on the implementation of ICT procedure (Identification and Authentication, Authorization of users, Confidentiality, Integrity and Availability (CIA), Non- repudiation and Auditability), On the enforcement policy, there should be guideline for ICT implementation and it's mandatory for government to come in to ensure consistency of the policy, guidelines of ICT implementation are not consistent due to lack of enforcement policy rules and regulations, enforceable laws which should be backed up by proper legislation. On compliance factor, much is expected that implementers should develop a positive attitude on the ICT implementation and must agree or conform to the terms of compliance. The Federal government of Nigeria must

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

promulgate legislation on cybercrime Act and offenders must be punished. Terms and condition of ICT usage must be strictly followed and all staff using ICT facilities must mandatorily sign an "Agreement form".

KEYWORDS: College of education, ICT policies, enforcement and compliance, ICT implementation and information security

I. INTRODUCTION

The Education system is one the sectors that Information and Communication Technology (ICT) policy initiatives in Nigeria has been targeting since 1988 (Adebowale & Dare; Yusuf, 2005, 2007). However, three decades later, little impact of ICT has been felt in this sector more especially in the Colleges of Education (Garba, Singh, Yusuf, &Ziden, 2013; Tella, 2011; Yushau&Nannim, 2018). This study examined the relevance of ICT policy implementation with a focus on the information security in Colleges of Education in Nigeria.

II. BACKGROUND OF THE STUDY

International Standards such as ISO 27002 are good starting point to implement ICT Security in any national system (Diver, 2007; Flowerday&Tuyikeze, 2016; Hong, Chi, Chao, & Tang, 2006; Hong, Chi, Chao, & Tang, 2003; Tuyikeze&Flowerday, 2014). In addition, (Bayuk, 2009) support the idea of using international standards as baseline framework because they increase trust in the organization. He stated that this is a reasonable approach as it helps to ensure that the policy will he accepted as adequate not only by higher education management but also by external auditors and others who may have stake in the organization security programme.

The main reason to develop ICT security implementation policy is to mitigate the various security risks that organization face (Iuyilceze&Flowerday, 2014). However, the process of developing the policy requires the organization first to identify and understand regulatory requirements that dictate creation of such policies before writing information security policy. (Avolio &Fallin, 2007) suggest that information security policy developers must familiarize themselves with penalties of non- compliance with laws. Therefore, it is necessary that colleges obtain legal advice that the policies are binding. Successful implementation of ICT security policies requires security awareness at all levels of the organization. ICT security awareness should be created through widely disseminated documentation, newsletter, emails a website, training programs and other notifications about security issues.

III. RELATED WORK

For ICT security implementation goals to be realized, users of IT resources should be trained to make them to be aware of potential security concern and understand their responsibility to report security incident and vulnerabilities.

(Okesola, Onashoga, &Ogunbanwo, 2016) observed that in Nigeria Information and Communication Technology (ICT) was introduced into Nigeria Education System curriculum in 2000. Prior to 1988 a lot of policy initiatives were developed to bring ICT security implementation into reality; this led to producing a

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

National ICT Policy draft in January 2012. In Nigeria colleges the Chief Information Security Officer (CISO) is charged with the responsibility of implementing the ICT security and must ensure compliance whereby if there are lapses disciplinary actions must be taken to sanction any criminality. The CISO must workwith the overall head of the organization. In Nigeria colleges efforts have been made to develop security policies program to address the overall ICT security implementation and IT security goals which apply to all IT resources within the institution. Program policies usually address confidentiality or service availability. Therefore, all program policies must meet and follow, comply with existing laws, regulations of state and federal policies.

Users at all levels should be trained in appropriate use of technology and developing appropriate user policies and enforcement of those policies. Despite the fact that Nigeria colleges of education have tried to ensure good ICT security implementation there are noticeable challenges such as vandalisation of ICT equipment, Slow internet, Erratic power supply, users do not familiarize themselves with ICT security policies and problem of sustainable maintenance of ICT equipment just to mention a few.

According to (Kearney & Kruger, 2013; Kruger & Kearney, 2008) ICT resources are important assets of any organization. Protection of these resources is equally important. To be able to protect themselves and their profitability many organizations have established information security awareness programs. In order for a security awareness program to add value to an organization and at the same time make a contribution to the field of information security it is necessary to have a set of methods to study and measure its effects.

One of the key defenses to address human oriented controls is the implementation of an information security awareness program. These programs are used to create and maintain security positive behaviour amongst employees and the goal of such programs would be to highlight the importance of information security systems and possible negative effects of security breach or failure. The importance of security awareness program is further emphasized in the BS7799: l where the objective of user training is given as to measure that all users are aware of information security treats and concerns.

Following the implementation of information security awareness program there is usually a normal business need to evaluate and measure the success and effectiveness of it. (Schlienger& Teufel, 2002) stated that evaluation should always be the final step in an information security management program in order to obtain information on efficiency and effectiveness of actions to define follow up actions and to justify investments in the program.

IV. THEORETICAL FRAMEWORK FOR THIS STUDY

I based my study on existing well-known theoretical frameworks in the domain of information security (Bell, 2006; McClelland, 2010).

The Protective Security Policy Framework (PSPF) (McClelland, 2010) highly put in practice by the Australian Government is committed to effectively manage the protective security risks to Government business and building interest trust confidence and engagement with the Australian people and their international partners. The Government requires agency heads to have in place effective protective security arrangement to ensure that respective agency's function to capacity.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

To achieve this, agencies are to apply the protective security policy framework and promote protective security as part of their culture.

The Bell-La Padula (BLP) model (Bell, 2006) is a model of computer security that focuses on mandatory and discretionary access control. A mandatory access control scheme is where one user/process (usually the system administrator or perhaps the operating system itself) creates and enforces the rules for access control. A discretionary access control scheme is one where the owner of a file can manipulate the access control permissions to their desire.

The first goal of the Bell-La Padula security model is to prevent users from gaining access to information above their security clearance. In other words, a user with "Classified" access (a low-level clearance) should not be able to read files marked as "Top Secret" (a higher level of secrecy), but someone with "Top Secret Access" should. The model calls this the Simple Security Property, because a naive security model might consider this sufficient. The way that the security model deals with this problem is through an Access Control List. Every file had an associated structure (called an Access Control List) that lists the permissions of every user in regards to the file. The language of the original model: "The Access Control List in Multics is a list of "(process, ring bracket)" pairs (for our purposes here, the Multics analogue of subjects) allow access to a segment (that is, an object) and the modes of access allowed."

The second goal is the protection of information containers rather than of the information itself. That is, a malicious program might pass classified information along by putting it into an information container labelled at a lower level than the information itself. In other words, there's nothing in the Simple Security Property to stop a malicious Top-Secret level user from reading information in one file, then copying that information into a new file which is able to be read by a user with a lower-level security clearance. To combat this 1mw, Bell & La Padula came up with the "property", which is described as "a subject at a given security level must not write to any object at a lower security level." In other words, you can only create documents of an equal or higher-level security than your access level. This property is called "write up"

V. METHODOLOGY

Based on the above discussed theoretical background, the study adopted a cross sectional survey design. This is a design where by data is collected at one point in time from the cross sectional of the study population (Creswell, 2012). In addition, the study employed both quantitative and qualitative approaches (Creswell, 2011). The choice for this approach was-based on the premise that when quantitative and qualitative methods are used in combination a more complete analysis would be obtained since they complement each other (Morse, 2003). Quantitative approach depends upon the collection of quantitative data such as statistics and percentages. This approach uses a number of methods and models such as time-series analysis and input-output analysis, and often it contains descriptive statistics and inferential statistics in order to test the raw data and to unveil the facts accordingly, in other words, it is the process of presenting and interpreting numerical data. The objective of quantitative research in this study was to employ theories, and hypotheses pertaining to the phenomena under research, quantitative method is widely used in social sciences such a economics, marketing, and political science hence it was deemed relevant in this study (Bryman, 2006).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

On the other hand, the qualitative approach is based upon developing a hypothesis, for example, based upon the actual scenario in the education sector. The qualitative approach relies primarilyon the collection of qualitative data in form of words, pictures, and objects. This method is employed in many different academic disciplines and traditional social sciences. The qualitative approach introduces information only on particular hypotheses and quantitative methods can be used to verify which of such hypotheses are true (Lazo, 2010). Additionally, it aims to gather in- depth understanding of human behaviour which involves extensive study of the claims made by the researcher according to the previously conducted work.

Study Population

In this research, the study population included the entire staff (teaching and non—teaching staff) of the selected colleges of education in Nigeria, 1,593 in total. The target population refers to the total number of subjects or the total environment of interest to the researcher (Onen, 2016). The target population of this study included only the staff members who worked in the ICT departments of the selected colleges of education in Nigeria. This was considered due to the nature of the research. They were170 in total and they included system administrators, ICT support technicians, ICT laboratory assistants and ICT support staff, Therefore, system administrators must be supportive and give attached departments full cooperation as they must work together as partners to move the organization forward.

This study involved systems administrators because they are charged with the role of installing, supporting and maintaining servers or other computer systems, and planning for and responding to service outages and other ICT problems within the college. Furthermore, ICT support technicians were involved in this study because they provide technical support and assistance for users of computer infrastructure and web technologies. They also undertake diagnosis and resolution of technical problems. Table 3.1 gives the summary of the target population.

Table 3.1 Sample of theTarget Population

Colleges of Education in Nigeria	Target Population			
	Systems Administrator	ICT Technicians	ICT Laboratory Assistants	ICT Support Staff
Federal College of Education, Zaria	1	2	1	6
Federal College of education (T), Bichi	1	3	3	3
Federal College of Education (T), Gusau.	1	2	3	8
Federal College of Education, Kano.	1	3	4	4
College of Education, Oyo (special)	1	2	2	3
Federal College of Education, Yola	1	1	3	4
Lagos State College of Education, Ijanikin	1	2	3	7
Federal College of Education, Okene	1	2	1	5
College of Education, Yenagoa	1	2	3	6
Federal College of Education, Omoku	1	2	2	4
FCT Zuha College of Education, Abuja	1	2	2	7
Subtotal	11	23	27	57
Overall Total				118

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Similarly, this study included the laboratory assistants because they coordinate scheduling of students and lecturers for the purpose of maintaining computer lab operations and activities, and instructing students and lecturers in computer lab technology and software applications. Lastly, ICT support staff were included in the study because they deal with the day to day issues of maintaining a trouble-free environment for effective use of ICT equipment, assisting staff and students to overcome any difficulties they may be experiencing e.g. printer failure, poor PC performance, etc., and performing daily checks on all ICT equipment to ensure it is unacceptable working order. The researcher used both simple random sampling (probability sampling) and purposive sampling (non-probability sampling) to select the above respondents.

Sampling Technique

According to (Johnson & Christensen, 2014), having established the actual sample size required, the researcher selected the most appropriate sampling technique to obtain a representative sample. Sampling technique basically refers to the method employed in obtaining the sample size for the research. According to (Mugenda & Mugenda, 2003) sampling technique is very necessary in any social study because it helps in answering questions pertaining to what the respondents were called upon to give answers to the research questions, whether the selected group of respondents is adequately representative of the population, how wide a coverage would be acceptable and other questions that would help the researcher in the selection of his sampling design.

According to (Saunfiers, Lewis, & Thornhill, 2007), five main techniques can he used to select a probability sample: simple random; systematic; stratified random; cluster; and multi—stage. Simple random sampling involves selecting the sample at random from the sampling frame using random number tables, a computer or an online random number generator; such as Research Randomizer (2008).

This study also employed non-probability sampling, that is, purposive sampling technique, first to select the Colleges of Education in the different States that make up northwest geopolitical in Nigeria. Secondly, the study used purposive sampling to select the ICT team from each of the selected Colleges of Education given their already small number. The method was used because it enabled the researcher to identify uniquely qualified respondents to provide needed information. The selection was based on expert knowledge of the particular problem of the research. This helped the researcher to select respondents who seemed to know more and work directly with the implementation of ICT policies and information security.

Data Collection Methods

The study adopted three methods of data collection, namely: questionnaire survey, interview survey and document analysis.
The questionnaire (structured questionnaire) data collection tool was employedbasing on the objectives hence targeting the system administrators, ICT support technicians, ICT laboratory assistants and ICT support staff to respond to questions regarding ICT policy implementation and information security. The tool was preferred because it is easy to administer, saves time and allows for doubts to be clarified on spot from many respondents (U. Sekaran, 2003).

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

The interview survey method was used to collect data from at least the systems administrators from each of the selected Colleges under survey. This method was helpful in collecting data regarding ICT policies. The researcher preferred this method because it enables the researcher to probe more and even read actions and expressions of the key informants (Jackson, 2009).

The documentary analysis method was also used to obtain information related to the study from a variety of written materials from scholars, and authors. Specifically, the researcher analysed ICT policies in each of the selected colleges and their information security mechanisms using a documentary checklist. This method was helpful to the researcher to establish facts, current trends, relationships, critics, gaps, and how the study would cover the gaps in addressing ICT policy implementation and its effectiveness in ensuring information security (Freebody, 2003)

VI. THE FINDINGS

This describes the analysis of data followed by a discussion of the research findings. The findings relate to the research objectives that guided the study. Data was analysed (SPSS) to identify, describe and explore the relationship between ICT policy implementation and information security of Colleges of Education in Nigeria. The researcher used five Likert scale as shown in the table.

Description of the respondents in the study: Demographic characteristics of the respondents

A descriptive summary of the 114 study participants has been presented in Table 4.1 below.Majority of the respondents were males (68.42%) and aged 20-29 years (51.75%). The highestproportion of respondents had attained Diploma level (45.6 1%) education and had I to 5 years(50.0%) experience in JCT information security. The highest proportion of respondents was ICTsupport staff (36.84%). Majority of the respondents had no special training in ICT information security (28.95%).

Access control mechanisms

Respondents were asked to provide feedback on the extent to which the respective Colleges of Education they work with have access control mechanisms. As to whether all College staff had access to computers, majority of the respondents strongly agreed (92.11%) while the minority agreed (7.02%) and those who strongly disagreed represented (0.88%). As to whether usernames and passwords were changed periodically, majority of the college ICT staff agreed (67.54%), followed by those who strongly agreed (26.32%) and only a few reporting not to be sure (4.39%) and disagreeing (1.75%). As regards all non-system administrator staff having limited access to ICT information from any computer, majority of the respondents strongly agreed (55.26%), followed by those who agreed (39.47%) and lastly those who weren't sure (5.25%).

Table 4. 1 Access Control Mechanism (ACM)

Variables	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
ACM1	1	0.88					8	7.02	105	92.11
ACM2			2	1.75	5	4.39	77	67.54	30	26.32
ACM3					6	5.25	45	39.47	63	55.26

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Terms and conditions of ICT usage

Respondents interviewed concerning terms and conditions of ICT usage in the respective Colleges of Education were 105. This too is one of the key components of ICT policy implementation. Pertaining to having a provision for all staff to sign an agreement on terms and conditions of using ICT facilities, only half of the respondents strongly agreed (50%) while the rest just agreeing (46.49%) and the least weren't sure (3.51%). As regards only employed staff having access to ICT facilities, the highest proportion strongly agreed (48.25%) and agreed (43.86%) with only(7.89%) reporting not to be sure. As to whether all terminated staff must return all ICT facilities in their possession to the college management, majority strongly agreed (64.91%) followed by those who agreed (28.95%) and lastly those who weren't sure (6.14%). Regarding the College reserving the right without notice to limit or restrict any individual's use and to inspect, copy, remove or otherwise alter data, files or system resource which is used in violation of college rules or policies is summarized in Table 3 below as well. Majority of respondents strongly agreed (65.79%) while the rest either agreed (32.46%) or weren't sure (1.75%).

Table 4.2 Terms and conditions of ICT usage (TCU)

Variables	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
TCU1					4	3.51	53	46.49	57	50.00
TCU2					9	7.89	50	43.86	55	48.25
TCU3					7	6.14	33	28.95	74	64.91
TCU5					2	1.75	37	32.46	75	65.79

Disaster recovery plans and mechanisms

Table 4.3 provides a summary of respondent's feedback when asked about disaster recovery plans and mechanisms in their Colleges of Education. When asked whether the turnaround time to receive a backup tape for recovery was a maximum of two hours, 51.75% of the respondents strongly agreed whilst43.86% agreed however 4.39% of the respondents were not sure. As regards backup information being given an appropriate level of physical and environmental protection consistent with standards applied at the main site, majority of the respondents strongly agreed (62.28%) followed by those who agreed (31.58%) and lastly 6.14% were not sure. Concerning whether backup media is regularly tested, where applicable to ensure that they can be relied upon for emergency use when necessary, the highest proportion of respondents strongly agreed (54.39%) and agreed (42.11%) with only 3.51% not sure. As regards restoration procedures being regularly checked and tested to ensure that they are effective and that they can be completed within the recovery time that has been allotted in operational procedures for recovery, the highest proportion of respondents strongly agreed (55.26%) and those that agreed (42.11%) with only 2.63% not sure.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Table 4.3 Disaster Recovery Plans and mechanisms (DRP)

Variables	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
DRP2					5	4.39	50	43.86	59	51.75
DRP4					7	6.14	36	31.58	71	62.28
DRP5					4	3.51	48	42.11	62	54.39
DRP6					3	2.63	48	42.11	63	55.26

Identification and authentication

This is one of the key aspects of information security. Information on how the colleges of education fared on this is summarized in Table 4.4. Concerning every staff having an independent identification code when accessing information from a computer, majority of the respondents strongly agreed (84.21%) with the minority agreeing (14.91%) as well as those not being sure (0.88%). As concerns every staff having a user account, username and password, majority of the respondents that strongly agreed were 50% while 48.25% agreed and those that were not sure and those that disagreed were represented by 0.88%.

Table 4. 4 Identification and authentication

Variables	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
IA1					1	0.88	17	14.91	96	84.21
1A2			1	0.88	1	0.88	55	48.25	57	50.00

Authorization

Different staff have different access privileges given to them by the system administrator. 65.79% strongly agreed with the lowest proportion reporting that they weren't sure (2.63%). Furthermore, with regards to all staff being registered so as to use ICT facilities, majority of the staff strongly agreed (55.26%) while 1.75% weren't sure.

Table 4.5 Authorization

Variables	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
AZ1					3	2.63	36	31.58	75	65.79
AZ2					2	1.75	49	42.98	63	55.26

Integrity

With regards to data being kept from being changed in unauthorized ways (IT1), majority ofthe respondents strongly agreed (80.70%) to this fact where as18.42% agreed and only 0.88% disagreed. As to whether data is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

ensured to be accurate and in good condition (IT2), the highest proportion of respondents agreed (57.02%), followed by those who strongly agreed as 33.33% then those who weren't sure were 9.65%. In addition, with reference to whether the system administrator encrypts vital information for security reasons (IT3), majority of the respondents strongly agreed (64.91%) with the rest either agreeing (28.07%) or not sure (7.02%).

Availability

With regards to information always being available at the time it's needed, the highest proportion of respondents who strongly agreed were 50.88% and those that agreed were 46.49% with only a minority not sure (2.63%). Pertaining to whether the system administrator ensures that the computing systems used to store and process information, the security controls used to protect it, and the communication channels used to access it are functioning correctly, majority of the respondents strongly agreed (64.91%). As concerning the college having very good network security mechanisms to prevent external attacks that might compromise data availability, the highest proportion of respondents who strongly agreed were 56.14% whilst those who agreed were 42.98%.

Table 4. 6 Availability

Variables	Strongly disagree		Disagree		Not sure		Agree		Strongly agree	
	Freq.	%	Freq.	%	Freq.	%	Freq.	%	Freq.	%
ATI					3	2.63	53	46.49	58	50.88
AT2					8	7.02	32	28.07	74	64.91
AT3					1	0.88	49	42.98	64	56.14

ICT policy implementation and information security

In order to study the association between ICT policy implementation and information security, the feedback of the respondents to respective questions used to evaluate each of the components of both ICT policy implementation and information security were averaged and a new scale generated. This scale ranked the performance of the various colleges of education ranging from being very unsatisfactory to being satisfactory based on self-reported responses of staff from the colleges interviewed. For respondents whose responses when averaged for a specific component of either ICT policy implementation or information security ranged from 1 to 1.8, the college was considered to have very unsatisfactory performance on that component. In detail, the categorizations included; very unsatisfactory (1 to1.8), unsatisfactory (1.81 to 2.60), fairly satisfactory (2.61 to 3.40), satisfactory (3.41 to 4.20) and very satisfactory (4.21 to 5.00).

Table 4. 7 Association between components of ICT policy implementation security and information

Variables	**Information security**		
Access control mechanism	**Satisfactory**	**Very satisfactory**	**n**
Fairly satisfactory	0.00	100.00	1
Satisfactory	8.33	91.67	12
Very satisfactory	5.94	94.06	101
Terms and conditions of ICT usage			

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

Satisfactory	10.00	90.00	10
Very satisfactory	5.77	94.23	104
Backup and recovery mechanism			
Satisfactory	18.18	81.82	11
Very satisfactory	4.85	95.15	103
Disaster recovery plans and mechanisms			
Satisfactory	66.67	33.33	6
Verysatisfactory	2.78	97.22	108

Table 4.7 above provides a summary of the association between the components of ICT policy implementation and information security. Concerning access control mechanisms, all colleges of education performed at least fairly satisfactorily. Furthermore, majority of the colleges with a very satisfactory access control mechanism had very satisfactory information security (94.06%). Regarding terms and conditions of ICT usage, majority of colleges with very satisfactory performance had very satisfactory information security (94.23%). Similarly, majority of colleges with very satisfactory backup and recovery mechanisms also had very satisfactory information security (95.15%). Likewise, majority of colleges with very satisfactory disaster recovery plans and mechanisms had very satisfactory information security (97.22%).

VII. DISCUSSIONS, RECOMMENDATIONS AND CONCLUSIONS

This section discusses the findings of the study in accordance to study objective and cross references them with empirical studies presented in the background of the study section above. Conclusion on major findings and recommendations are subsequently presented.

Discussion -

It was found that ICT policies were satisfactorily implemented in most of the surveyed Colleges of Education. This was attributed to the fact that respondents indicated that variables such as access control mechanism, terms and conditions of ICT usage, backup and recovery mechanism, disaster recovery plans and mechanisms were satisfactorily implemented ICT policies in their colleges.

This finding of the study is consistent with (Peansupap& Walker, 2006) work. There should be an ICT implementation process for providing learning that concurrently integrates both technical and organizational support. The authors further explained learning and training content coupled with delivery quality may be important constraint issues. Basic ICT training can be integrated into ICT policies so that users can be aware of concepts and benefits of technical know-how. Not until such level of literacy is attained among users, then no high level of ICT innovation in their work processes.

In a related development ICT implementation and adoption is a management intensive activity that managers should reframe. Implementation on expectations create small win and reduce any conflict of interest. However educational policy makers are in unique position to bring about change. This is illustrated in a study of 174 ICT supported innovative classroom in 28 countries (Kozma, 2005). In 127 cases there were explicit connection between the innovation and national policies that promoted the use of ICT (Jones, 2003). But while the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

introduction of ICT policy is necessary for change. It is not sufficient, to result in its implementation or impact (Tyack & Cuban, 1995) Policies can of course fail to succeed and this happen when; (i) they are viewed as mere symbolic gestures, (ii) when teachers actively resist policy based change that see as imposed from the outside without their input or participation, (iii) when they do not have explicit connections to instructional practice (e.g. focus on hardware rather than their relationship to pedagogy), and (iv) then there is lack of programme and resource alignment to the policies intensions (Cohen & Hill, 2001; Tyack & Cuban, 1995).

According to (Phaopeng, 2010) posts that the term policy implementation has been defined by many scholars in association with the meaning of public policy implementation can be viewed only from a particular perspective but also from various dimensions as a number of remarkable scholars. Phaopeng 2010 in his findings further observed that users name and passwordsbeing changed periodically (at most monthly) and only authorized person having access to specific details of given information.

VIII. CONCLUSION

The study established that ICT policies have been implemented to a great extent in most of the surveyed colleges of education. Similarly, the most basic security mechanisms have been implemented for example the use of password and usernames. In the same light the implementation of ICT policies was found to significantly affect the level of information security. This is because establishing access control mechanisms ensured data confidentiality, integrity, availability, none-repudiation and auditability of information. Defining terms and conditions of using college ICT facilities and services from different categories of users help to ensure data confidentiality and availability and shows good association between ICT policy implementation and information security in terms of performances and developing and implementing appropriate backup and recovery mechanisms for institutional data that helps to ensure data availability and developing and implementing ICT disaster recovery plan to ensure data availability.

All in all, therefore it can be concluded that good implementation of ICT policies is a prerequisite for high level performance of information security, However, if policies are not well implemented to cater for information security aspects of the co1leges then the likelihood of ensuring that the five pillars of information security are well addressed will be low.

Recommendations

The following recommendations were drawn as way forward to achieve viable ICT policy implementation and information security.

a. ICT personnel need to be trained on regular basis to sharpen and enhance their knowledge on new threats to information security. This can be done through ICT workshop retreats, seminar and symposium.
b. The staff and students must be regularly supported guided and trained by ICT personnel on how to ensure information security of ICT facilities. They can be taught about topics such as antivirus installation, passwords, portable media devices, back up, social media internet usages, internet of things hence scams and email scams.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 9, Issue 3, March 2020

c. The Federal Government of Nigeria must promulgate legislation on cybercrime act and offenders must be punished.
d. Terms and condition of ICT usage must be strictly followed. All staff using ICT facilities must mandatorily sign an "agreement form "for them to have access to the ICT facilities.
e. The Federal Government of Nigeria must embrace the new technology of Public Key Infrastructure (PIG) of encryption of information in ICT systems.

REFERENCES

1. Adebowale, 0. F., & Dare N. 0. Teachers' Awareness of Nigeria's Educational Policy on 1CT and the use of ICY in Oyo State Secondary Schools. International Journal of Computing and ICT Research, 60), 84-93.
2. ATSB, A. T. S. B. Reliability of Robinson R22 helicopter belt drive system ATSB. ATSB Transport Su/L4y Report, Aviation Occurrence Investigation, AJ-2009-038, 2013.
3. Bayuk, J. I-low to Write an Information Security Policy. Computerworld. Bell, D. F. (2006). Looking back at the Bell-La Padula model (Vol. 2005), 2009.
4. Creswell, J. W.Educational Research: Planning, Conducting and Evaluating Quantitative and Qualitative Research. 4thEdn, Pearson Education, Boston, ISBN-lU: 0132613948, pp: 650, 2011.
5. Diver, S. Information Security Policy - A Development Guide for Large and Small Companies. SANS Institute. South Africa., 1—43, 2007.
6. Flower&y, S., &Tuyikeze 1. Information security policy development and implementation: The what, how and who. Computers & Security, 61, 169-183. doi: lO.10l6/j.eose.2016.06.00, 2016.
7. Garba, S. A., Singh, T. IC R Yusuf, N. B. M., &Ziden, A. A. An Overview of ICY Integration in Nigerian Colleges of Education and the Implications on Social Studies Pre-Service Teacher Training Programme: A Review of the Literature, Journal of Education and Learning, 70), 3 5-42, 2013.
8. Johnson, R. B., & Christensen, L. Educational research: Quantitative, qualitative, and mixed approaches, Fifth edition. SAGE Publications, 621, 2014.
9. KLan, K. Present status of information communication technology (ICT) and infrastructure facilities in high court libraries of India. International Journal of Library and Information Science, 3(5), 81-87, doi:10.5897/IJLIS1 1.081, 2012.
10. Mugenda, 0. M., & Mugenda, A. G. Research Methods: Qualitative and Quantitative Approaches. Nairobi: Africa Center for Technology Studies, 2003.
11. Olcesola, J. 0., Onashoga, A., &Ogunbanwo, A. An investigation into users' information security awareness on social networks in south western Nigeria. SA Journal of Information Management, 18(1). doi: s//cojg/l0.4102/sajim.v18i1.721, 2016.
12. Peltier, T. R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, FL: Auerhach publications2012.
13. Yushau, B., &Nannim, F. A. lOT Facilities and their Utilization for Educational Purpose in Nigerian Universities: A Review of Literature from 2004 to 2018. ATBU Journal of Science, Techt2olog & Education. 6(1), 2018.