

The purpose of this study was to assess the maintenance of electronic records at Africa University. Maintenance of electronic records includes storage, policies, procedures, security and classification. A case study involving a sample of 33 employees from 3 departments was undertaken. Interviews with the Bursar, Librarian and the ICT Director were conducted while questionnaires were distributed to the Library staff, ICT staff and the Accounts office. The study revealed that the maintenance of electronic records at Africa University is not effective.

15 **1.0 Introduction**

16 According to IRMT (2004) Electronic records is recorded information, documents or
17 data that provide evidence of policies, transactions and activities carried out in e-
18 government and e-commerce environments. The National Archives of Australia Digital
19 Recordkeeping Guidelines (2004:13) note that electronic records include word-processed
20 documents, spreadsheets, multimedia presentations, email, websites and online
21 transactions. Electronic records can be found in many systems throughout the
22 organization-including databases and business information systems, shared folders and
23 hard drives. According to the Victorian Electronic Records Strategy (2002), electronic
24 records are evidence of organizational activities and are generally the computerised
25 versions of traditional paper records. Sources of electronic records range from desktop
26 publications such as Word, Excel, and email, to corporate applications such as financial
27 systems, human resource systems and corporate databases.

Electronic records management may be defined as that part of records management that deals with records in electronic form. According to Johnston (2005:132) this includes 'the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities'.

33 The unprecedented development and diffusion of electronic computers and related
34 Information and Communication Technologies (ICTs) has created a situation where
35 atAfrica Universityalmost every employee has a computer on his or her desk. The
36 availability of computers implies that at Africa University volumes of electronic records
37 are created on a daily basis. There is, therefore, a need to assess how these data are
38 maintained in terms of policies, procedures and practices.

39

40 **2.0 Research Problem**

41 Taking advantage of the unprecedented development and diffusion of electronic
42 computers and related Information and Communication Technologies (ICTs) Africa
43 University has automated most of its operations. This implies that at Africa University
44 volumes of electronic records are created on a daily basis. However, little is known on
45 the strengths and weaknesses of current electronic records maintenance policies,
46 procedures and practices at Africa University. This paper aims at filling this knowledge
47 gap.

48

49 **3.0 Literature Review**

50 According to Darlington (2003:1) there has been considerable debate about the
51 development of the electronic records management as an academic discipline. However,
52 there seems to be an emerging consensus about the existence of a body of theoretical
53 knowledge tackling issues of document authentication, archiving, permanent storage,
54 inactive storage, disposal, information science and principles behind practices such as
55 retrieval, maintenance, active storage and indexing. All these principles and practices are
56 affected by the use of Information and Communication and Technologies (ICTs) in
57 practices such as handling intangible records, physical control and data transformation.
58 Michalson (2005) describes records maintenance regimes according to their ability to
59 sustain or preserves records, along with the means to identify and retrieve them easily.
60 The objective of an effective records maintenance system is to keep authentic, reliable
61 and usable records.

62

63 Electronic Records Management (ERM) has become an essential business activity and an
64 element of compliance with regulation in many countries. King (1997:656) pointed out
65 that many business transactions depend on the proper creation and maintenance of
66 recorded information. The medium on which the recording of information could be done

67 may be paper, microfilm, audiotapes, videotapes, photographs, slides, or any computer
68 readable medium such as computer tapes or disks, compact disks and optical disks. Gold
69 (1995:1) characterized an organization's management of its records as the corporate
70 secret weapon and the winning strategy that gives the organization the competitive
71 edge. Mnjama (2002:34) explains that, despite the fact that universities are continually
72 being called upon to function in a business-like manner in order to be self-sustaining and
73 to remain competitive, they overlook the enormous advantages that proper records
74 management practices could contribute to the achievement of their objectives. Asogwa
75 (2012) observed that paper and electronic records maintenance systems should contain
76 metadata (descriptive and technical documentation) to enable the system and the records
77 to be understood and to be operated efficiently, and to provide an administrative context
78 for effective management of the records. The record-keeping system, whether paper or
79 electronic, should include a set of rules for referencing, titling, indexing and, if
80 appropriate, security marking of records.

81

82

83 State Records NSW (2004) defines records maintenance as a range of processes and tasks
84 which aim at (1) protecting records from unauthorised access, loss, destruction, theft or
85 disaster and (2) preserving the integrity of the records over time. Records maintenance
86 implies also keeping the records accessible when they are needed. Records maintenance
87 includes activities such as (1) storage of active records i.e. establishing and managing
88 facilities for records in all formats in or close to office or other work areas; (2) storage of
89 electronic records i.e. use of online and offline data storage devices; (3) preservation i.e.
90 establishing and monitoring appropriate environmental conditions for storing different
91 types of records, implementing safe handling practices, preventing damage to or misuse
92 of records, or transferring records to a different medium (from paper to microfilm, for
93 instance); (4) migration i.e. adapting records to new media generated by technology
94 change in order to keep them accessible over time. This step includes documenting
95 migration actions. (5) vital records i.e. identifying records and recordkeeping systems
96 critical to the functioning of an organisation and developing strategies to reduce the risks
97 of losing or destroying these records; (6) disaster management i.e. identifying and
98 assessing the risks of disasters affecting records, developing strategies to prevent and
99 respond to the disasters and devising means of recovering the records in cases of
100 destruction, theft or damage.

101 There are two types of records that can be electronically stored, namely, physical records
 102 and virtual records. According to Duranti (1996) physical records are recording the
 103 location of a record and this is typically managed as collections as collections of boxes
 104 rather than individual documents. This approach is used mostly because of the
 105 difficulties of adding document level information to a database combined with typical
 106 lack of resources for this purpose. Physical records are electronic and stored on media
 107 such as CDs, DVDs, CDROM, USB, External Hard drives and any storage device with a
 108 computer to be accessed. Virtual records, on the other hand, are records that are not
 109 physically stores in a certain media but can be virtually stored on the servers and on
 110 internet. A virtual record consists of pointers to data residing in different locations within
 111 a database, or in multiple databases. While it is possible to see on a computer monitor the
 112 records resulting from the assembly of those data in a meaningful form, these records do
 113 not exist as such until their components are actually joined together in an inextricable
 114 way, that is, until the content of the document is explicitly articulated in a fixed
 115 form.(Duranti, 1995)

116

117 The implementation of these models and the maintenance of various types of records
 118 need to be supported by adequate policy. Policy development has been emphasised by
 119 many authors as key to good records management (Kahn 2004:3). Record maintenance
 120 policy would clearly set out the organisation's expectations regarding retention,
 121 individual roles and responsibilities, ownership, control, classification of different
 122 categories of content and privacy (Myler and Broadbent 2006:3). The failure to capture
 123 and preserve electronic records in eastern and southern African institutions of higher
 124 education have been attributed to lack of policies and procedures, among other factors
 125 (Wamukoya and Mutula 2005:74). Norris (2003:3) reports that not many higher
 126 education institutions in the United Kingdom had well defined and active e-mail
 127 archiving policies in place. In the United States, findings from Duke University show
 128 that lack of defined policies resulted in different capabilities and different levels of e-
 129 mail management, backup, security and privacy usage among faculties (Tibbo and Pyatt
 130 2006:3) Similar problems have been reported at Loughborough University (Norris
 131 2003:3) and at the University of KwaZulu-Natal (Chinyemba and Ngulube 2005:13).
 132 Myler and Broadbent (2006:7) highlighted that once policies have been established the
 133 roles and responsibility of each individual in the organisation needs to be clearly set out
 134 and efforts must be made to ensure that everyone involved understands their roles and

responsibilities thoroughly for instance, an individual using e-mail would be expected to identify and categorise e-mail records of value, apply consistently relevant contextual information and metadata, and ensure their integrity. The institution on the other hand has the responsibility of providing guidance on categories of e-mail to be retained and retention schedules, provide viable mechanisms for archiving of records, training and support to staff and students. Norris (2003:3) emphasizes the duty of care whereby consideration needs to be given to how people do their jobs, how authority is delegated and the separation of responsibilities to reduce collusion and potential fraud.

143

According to Harris (2003) to electronic records maintenance at universities should operate within the framework of policies, rules and procedures that give guidance to practice. The purpose of clear policies and procedures is to provide an environment conducive to proper records maintenance. This is particularly important in an environment, such as the universities, where the responsibility for electronic records maintenance is distributed among the individual units with little or no centralized control. Therefore adherence to proper policies and procedures is essential to provide broad guidelines in which procedures may be developed in the operations of the organization. Robek (1995:7) pointed out that “the standardization of clear policies and procedures is to be realized, and then proper controls must be applied to records during the different stages they pass through from creation to disposal”. This ensures that records maintain their value as authentic evidence of activity throughout their life cycle. Therefore the existence of a policies and procedures is critical in an organization such as Africa University.

158

However, putting in place policies is not enough. For effective electronic records maintenance, all the people involved need to comply with the policies and regulations. According to Myler (2006:2) there is increasing pressure on organizations to ensure that their electronic records meet legislative requirements of authenticity, reliability and originality (Section 25 (Part 1, chapter 3) of the South African Electronics Communication and Transactions(ECT) Act (South Africa Government, 2002) clearly regulates document retention, retrieval of critical data and unsolicited communications. Thelwall (2008:1) highlighted that there are many cases where members of online social networks have been involved in inappropriate acts, for example posting of obscene photos, disclosure of personal details of others and use of abusive language (Greenop

2007:1) acknowledges that literature suggests several factors influencing regulatory compliance, for instance economic factors such as potential legal/illegal gains and cost of compliance. Mayne (2006:1) added that “the cost of compliance in electronic records maintenance is high or perceived to exceed potential liabilities.” Therefore compliance fails if regulated entities lack cognitive capabilities, understanding or ability to address environmental influences (psychological factors), compliance of electronic records maintenance may fail.

176

177 **4.0 Research Methodology**

178 **4.1 Research Design**

179 In this study the researcher used a case study design.

180 **4.2 Population and Sampling Techniques**

181 The population was the entire Africa University staff since they all generate electronic records on a daily basis. However, purposive sampling was used to select three departments which are key in the management of electronic records. These departments include Information and Communication Technologies (ICTs), the library and the Accounts office.

186

187 **Table 4.2 Table of sampled population**

	Total Population	Total Sample
Heads of Departments	3	3
Library Staff	10	3
Accounts office Staff	5	2
ICT Staff	15	6
Total	33	14

188

189 **4.3 Research Instruments and Data Collection Procedures.**

190

191 25 questionnaires were distributed to staff in the three selected departments while in
192 depth interviews were respectively conducted with the Bursar, Librarian and ICT

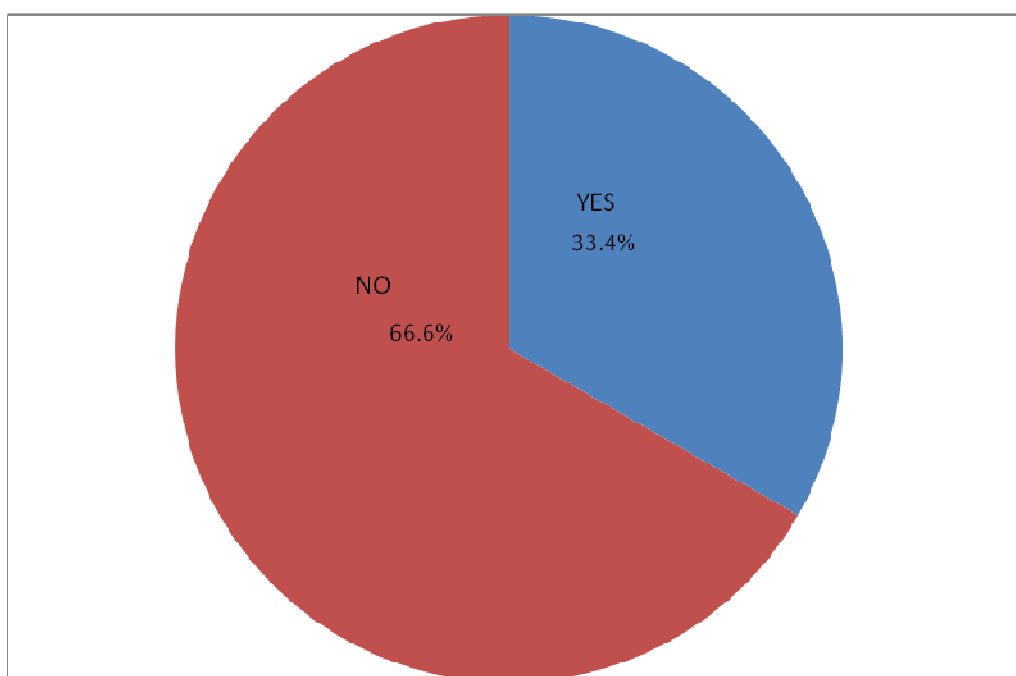
193 Director. Permission to conduct the research was sought for and granted in writing by the
194 University Registrar.

195 **5.0 Findings and Presentation**

196 **5.1 Awareness of Electronic Records Maintenance Policies and Procedures**

197 Figure 5.1 below shows that 8 (33, 4 %) respondents indicated that there was electronic
198 records maintenance policies and procedures. The highest number, 16 (66, 6%),
199 indicated that there was no policies and procedures that are followed in the maintenance
200 of electronic records at Africa University.

201 **Figure 5.1: Electronic Records maintenance policies and procedures awareness**

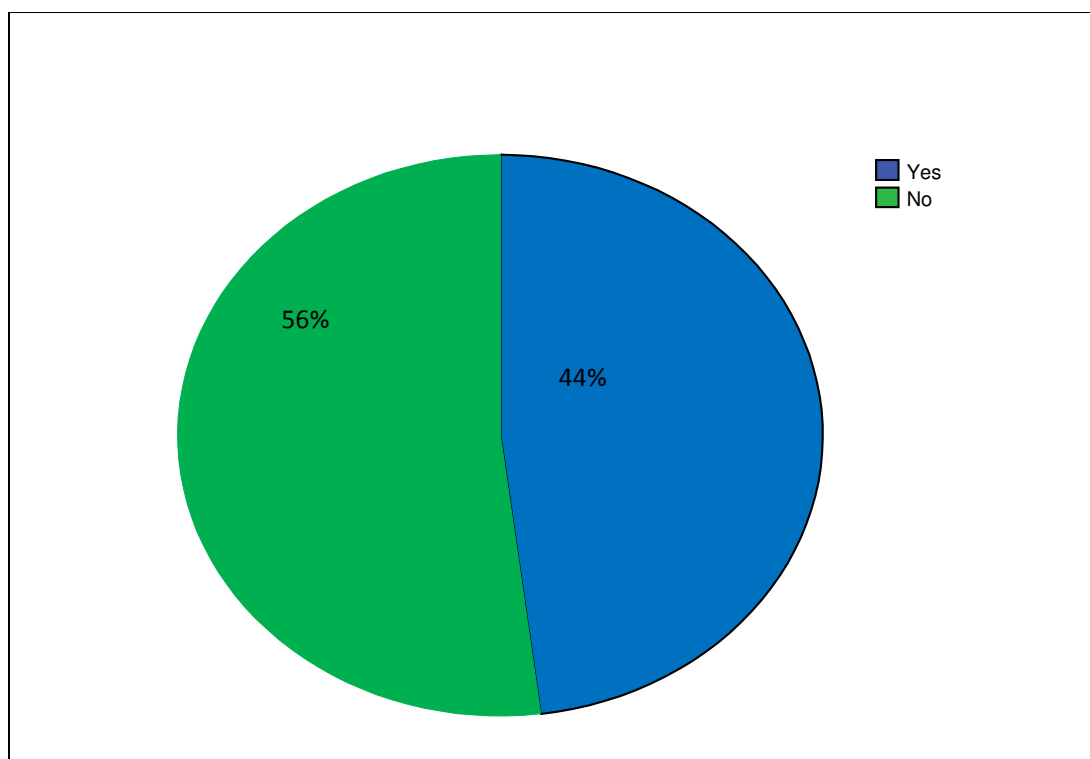


203 From the interview it has been gathered policies and procedures are there but they are not
204 always being followed by the staff owing to poor supervision. The problem, therefore,
205 poor dissemination of information on electronic records policies and procedures.
206 Concerning the importance of policies and procedures in the maintenance of electronic
207 records. The majority, 20 (55, 6%) were of the view that these policies and
208 procedures maintain the standards and guide electronic records administrators in the
209 proper ways of maintaining the records. However only four (11, 1%) pointed to the fact
210 that records will be preserved in maximum security.

211 5.2 Security Systems in Place for Protecting Electronic Records

212 From all the respondents, only (11) 44% respondents indicated that there are security
 213 systems in place for the electronic records while (14) 56% mentioned that there are no
 214 security systems in place. The results showed in fig 5.2 below demonstrate that the
 215 security systems of electronic records maintenance were unsatisfactory. When looking
 216 closely at these results, the researcher noted that there are security systems in place for
 217 safeguarding electronic records but there might be lack of information awareness to staff.

218 **Figure 5.2 Security Systems in Place for Protecting Electronic Records**



219
 220 Table 5.2 below reveals the reasons most respondents stated on the importance of
 221 security systems. 21% (3) staff indicated that security systems are important for limiting
 222 unauthorized access to electronic records, while 21% also cited that it is also important in
 223 daily backups of the systems so that records are not fraudulently altered. Security
 224 strategies including securing databases (28%) while keeping passwords safe (21%). 7%
 225 suggested that electronic records would be safer if there was an offsite back up system.

226

227

Respondents Suggestions		Frequency	Percent	Valid Percent	Cumulative Percent
	Limited rights to electronic records	3	12.0	21.4	21.4
	daily backups	3	12.0	21.4	42.9
	database security	4	16.0	28.6	71.4
	Safekeeping of passwords	3	12.0	21.4	92.9
	Protecting of offsite backup media	1	4.0	7.1	100.0
Total		25	100.0		

228

229

230

231 5.3 Restrictions of the Access to the Sever Room

232

233 All respondents indicated that the restriction of access to the server room is a key
 234 security measure. From the interview with the ICT director, it was highlighted that staff
 235 who are authorized to enter the sever room have to use a log book that indicates the time
 236 they have entered the server room and the time they will be out. The ICT Director
 237 pointed out that restrictions of access to the sever room minimizes the possibility of
 238 tempering with the servers by the unauthorised personnel and minimises the pilferage of
 239 electronic media. The University Librarian also highlighted that restriction of access to

240 server room protects the confidentiality of records that contains vital institutional
 241 information. The Bursar highlighted that the restriction of access to the server room is
 242 crucial as it also protects media that contains financial and accounting records of the
 243 institutions and minimizes deletion of records either through human error or fraudulent
 244 activity. The ICT Director is aware of the crucial role his department has to play in the
 245 effective security of electronic records at the University. He indicated his willingness to
 246 implement a computerised security system of the sever room. From the questionnaire,
 247 the researcher noted that the staffs have knowledge on the security features for the server
 248 room restriction as the majority of them had cited different reasons for server room
 249 restrictions.

250 **5.4 Backup of electronic records**

251

252 As shown in Figure 5.4 below 24 %(6) of the respondents indicated that backup of
 253 electronic records is done every day, while 48 %(12) indicated that backup is done
 254 weekly. The other 24% (6) indicated that they do back up monthly and 4 %(1) has
 255 indicated that it is done yearly. From these results it showed that backup of electronic
 256 records seems not to be consistent. There is no written standard operating procedure for
 257 the backup of the electronic records that indicates the schedule for backup. Therefore
 258 there is need for supervision for all staff that are administering the maintenance of
 259 electronic records in order to come up with a proper back up policies and procedures that
 260 will be followed by all electronic records administrators.

261

262

263

264

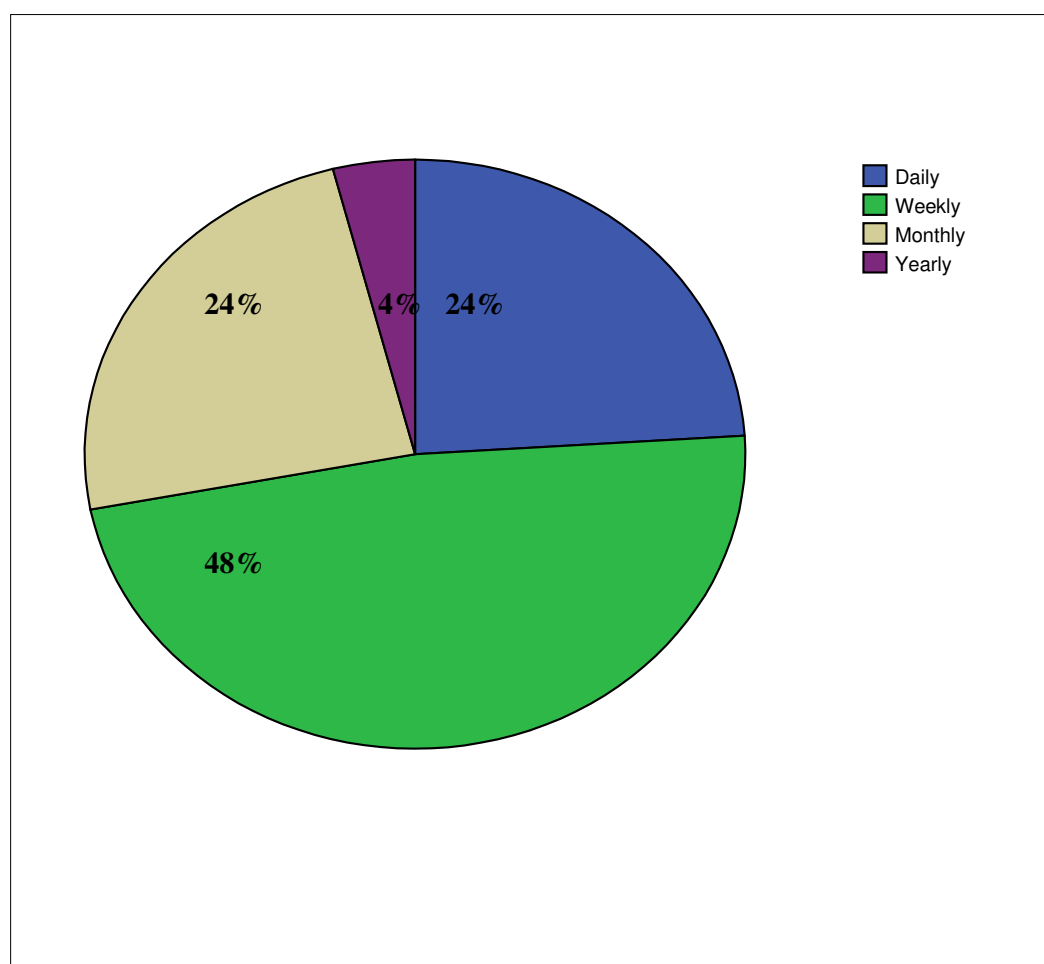
265

266

267

268

269 **Figure 5.4: Backup of Electronic Records**



271

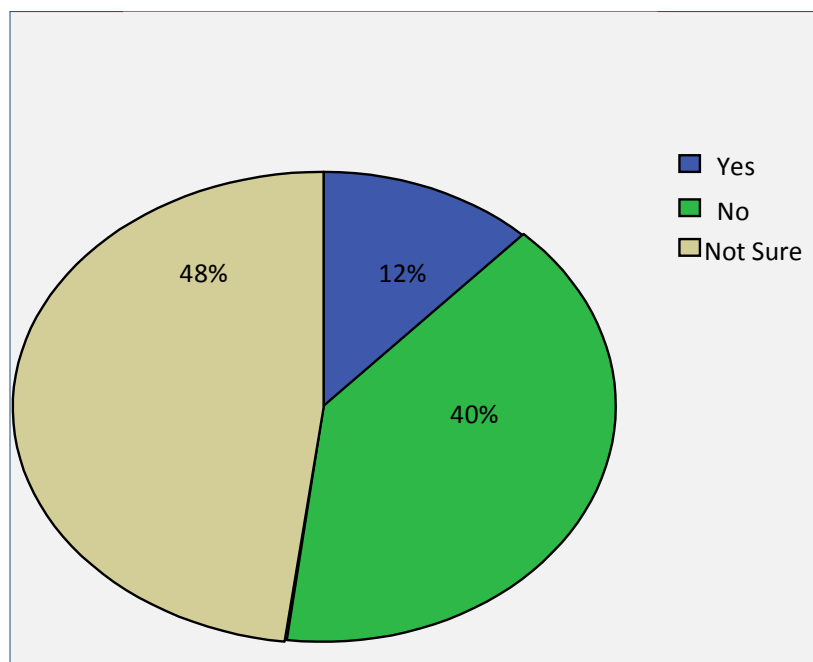
272 **5.5 Disaster Recovery Plan**

273

274 As shown in fig 5.5 below, three respondents (12%) indicated that Africa University
 275 have a disaster recovery plan to protect electronic records, while 40 %(10) indicated that
 276 there is no disaster recovery plan and the other 48 %(12) are not sure if there is a
 277 disaster recovery plan or not. Looking at the responses from interviews and the ones
 278 from other respondents, it might be clearly said that the institution does not have a
 279 Disaster Recovery Plan to protect electronic records. However, there might be a disaster
 280 recovery plan at Africa University but probably because it is not communicated to the
 281 staffs, most people might not be aware of its existence. This shows that there are
 282 limitations in the way the institution is disseminating information. Therefore,

transparency in the way of disseminating information should be encouraged so to promote awareness at the institution.

Figure 5.5 Disaster Recovery Plan



6.0 Conclusion

The study revealed that there is no effective maintenance of electronic records at Africa University. Staffs are not aware of existing policies and procedures although access to the server room is restricted. The staffs are aware of the importance of security measures such as security databases, upholding passwords and keeping off site backup systems. However, at the implementation level, are discrepancies in the regularity of backup which indicates that either there is clear policy or the policy which is not there is not consistently implemented. Most staff are not aware of the existence of a disaster recovery plan.

REFERENCES

- Asogwa, B.E. (2012) "The readiness of universities in managing electronic record: a study of three federal universities in Nigeria", *The Electronic Libraries*, in press.
- Chinyemba, A. and Ngulube, P. 2005. "Managing Records at Higher Education Institutions: A Case Study of the University of KwaZulu-Natal, Pietermaritzburg

302 Campus. South African.” *Journal of Information Management* 7 (1)
 303 <http://www.sajim.co.za/peer86.7nr1.asp>. (Accessed 10 October 2013).
 304
 305 Darlington, J., Finney, A. and Pearce, A (2003) *Domesday Redux: The Rescue of The*
 306 *BBC Domesday Project* Vidodiscs.Ariane <http://www.ariadne.ac.uk/issue36/tna/>
 307 Accessed 12 September 2013
 308
 309 Duranti Luciana and Heather MacNeil, (1996) “The Protection of the Integrity of
 310 Electronic Records: An Overview of the UBC-MAS Research Project,” *Archivarial*,
 311 Vol.42 (Fall 1996): 64
 312
 313 Duranti Luciana and Terry Eastwood, (1995) "Protecting Electronic Evidence: A
 314 Progress Report," *Arclzivi&Conzputer*5, no. 3.
 315
 316 Gold G. (1995) *How_To Set Up and Implement a Records Management System*. New
 317 York: American Management Association.
 318
 319 Harris, V. (2003) The challenges of preserving electronic memory over time. Paper read at
 320 Electronic Records Management Conference, Sandton,
 321 SA,<http://www.jisc.ac.uk/media/documents/publications/recordsmanbriefin> (Accessed 30
 322 September 2013)
 323 IRMT (2004) *The E-Records Readiness Tool*. London: International Records
 324 Management Trust.
 325
 326 Johnston, P and Bowen D. (2005) “The Benefits of Electronic Record Management
 327 Systems: A General Review of Published and Some Unpublished Cases” *Records*
 328 *Management Journal* 15(3) 131-140
 329
 330 Kahn, R.A. 2004. “Records Management & Compliance: Making the Connection.”
 331 *Information Management Journal* 38 (3):28–36.
 332
 333 King L.A (1997) “Are You Managing Your Vinyl Effectively?” *Management Decisions*
 334 35 (9): 656-659
 335 *Magazine Australia*. <http://www.scmagazine.com.au/feature/>

- 336 Mayne, M. (2006) “How Are Businesses Facing Up to The compliance Challenge?” *SC*
337
- 338 Michalson L. AND Hughes B (2005) *Guide to the ECT Act* (Online). Available [www](http://www.michalson.com)
339 <http://www.michalson.com> (Accessed 10 September 2013)
340
- 341 Mnjama N M. (2002). “Managing university records”. *ESARBICA Journal: Journal of*
342 *the Eastern and Southern Africa Regional Branch of the International Council on*
343 *Archives* 21:32-40
344
- 345 Myler, E. and Broadbent, G. 2006. “ISO 17799: Standard for Security” *Information*
346 *Management Journal* 40(6):43–52.
347
- 348 National Archives of Australia (1998). Archives advice 24: *Distributed Management of*
349 *Electronic Records*. [Online] <http://www.naa.gov.au> (Accessed 19 September 2013)]
350
- 351 National Archives of Australia (2004) *Guidelines for Creating, Managing and Preserving*
352 *Digital Records* www.naa.gov.au/recordkeeping/er/guidelines
353
- 354 Norris, M. 2003. *Records management and e-mail*. [http://www.dcc.ac.uk/events/ec-](http://www.dcc.ac.uk/events/ec-2006/EC_emailarch-rep.pdf)
355 [2006/EC_emailarch-rep.pdf](http://www.dcc.ac.uk/events/ec-2006/EC_emailarch-rep.pdf) (Accessed 18 September 2013).Page 14 of 15
- 356 Robek M.F Brown, G.F. and Stephens, D.O. (1995) *Information and Records*
357 *Management: Document-Based Information Systems*. New York: Glencoe/McGraw-Hill.
358
- 359 State Records NSW (2004) Standard on Full and Accurate Records. Standard No. 7.
360
- 361 State Records NSW (2004) Standard on Managing a Records Management Program.
362 Standard No. 8.
363
- 364 Thelwall, M. 2008. *Electronic policies and procedures online pages*. *Corpora*, 3(1).
365 (Accessed 20 September 2013).
366
- 367 Tibbo, H.R. and Pyatt, T. 2006. Email management, electronic records, and beyond.
368 [Online]. Available: <http://www.ils.unc.edu/digitaldesktop> (Accessed 17 September
369 2013).

- 370 Victorian Electronic Records Strategy (2002) Electronic Records Strategy, Melbourne,
 371 available at: www.provi.vic.gov.au/vers/standard/standard/3.htm (accessed 21 September
 372 2013)
 373
 374 Wamukoya, J. and Mutula, S.M. 2005. Capacity-building requirements for e-records
 375 management: the case in east and southern Africa. *Records Management Journal*
 376 15(2):71–79.