Security measures for digital archives curated through open-source software in South Africa

Mahlatse Shekgola[1]
shekgmm@unisa.ac.za ORCID: 0000-0003-2494-3232-76

Received: 22 May 2025
Accepted: 15 January 2026

Implementation free of open-source software (FOSS) can provide security for digital curation of archives these governmental bodies. As such, FOSS solutions for digital curation comprising of Archivematica, Access to Memory (AtoM), and DSpace are widely used by various archival institutions due to their flexibility, cost effectiveness, community support, and lack of licensing fees. This study explores security measures for digital archives curated through open-source software in South Africa, with the view of proposing strategies to enhance utilisation of free open-source software. The study adopted a qualitative research approach to collect data through interviews with purposively selected participants from national government departments, National Archives and Records Services of South Africa (NARSSA), and State Information Technology Agency. The findings of the study indicate that despite policy recommendation to use FOSS solutions, many governmental bodies are already locked into proprietary ecosystems, making difficult and expensive to migration. This make their data and workflows to be locked in on non-interoperable systems. The study culminates by outlining strategies that may be used ensure security of digital curation of archives through FOSS by government departments (creating agencies), as well as national archives (archival institution).

Keywords: digital curation, legislative framework, FOSS, proprietary software, South Africa

1 Introduction

Curation of archives in digital platforms ensures preservation and provision of access to valuable cultural, historical, and institutional information. In South Africa, digital archives are mostly managed through proprietary software despite the country having passed an open-source software policy in 2003. This continue to occur even when FOSS is widely lauded for its security capabilities when compared to proprietary software, especially in the sphere of archives and records management (Drake 2017). Moreover, as reported by Shekgola, Maluleka and Rodrigues (2021) and well as Ngoepe (2017), many governmental bodies, including national government departments lack knowledge of the South Africa's FOSS policy for governmental usage. Hence the slow and low adoption and implementation rate of the policy even in the area of archives and records management (Ngoepe 2017). Security of digital archives through open-source software provides a cost-effective and flexible way to safeguard vast amounts of data against possible cybercrimes, viruses, and inaccessibility of materials.

FOSS can provide more secure, dependable, and less costly technology when it comes to security. According to Karume and Mbugua (2012), this is because FOSS products provide users with the option of a detailed review of the source code, giving users the ability to fix problems themselves without having to wait for the vendor. On the other hand, proprietary products that are often rented tend to be packed with security vulnerabilities (Buffett 2014). Hence, according to Techopedia (2012), Linux (a FOSS operating system) is perceived to be the leading technology because it is seen as more dependable and safer than Microsoft Windows (proprietary operating system). Therefore, the attainment of the Linux operating system (for example) makes the concept of FOSS attractive to various organisations that deal with ICT activities.

In the South African context, where resource constraints often play a role, leveraging FOSS solutions for digital curation aligns with the principles of ensuring accessibility, retrievability and usability of records. As supported by Chen, Fu, Sun, Bilgihan and Okumus (2019) protecting digital archives requires a holistic approach encompassing access controls, encryption, network security, and compliance with relevant laws and regulations. Such protection is key to counter constant security threat of cyber-attacks, data breaches, and evolving security challenges. Failure to address security of digital archives may poses a serious concern for governmental bodies including the National Archives and Records Services of South Africa. Lack thereof robust security measures may result in inaccessibility of materials, theft, alteration, and deletion of records by authorised and unauthorised user. Hence the implementation of FOSS solutions may provide safety measures to curb the above-mentioned concerns and aid these governmental bodies to preserve significant, historical, and sensitive archives.

1. Mahlatse Shekgola is Senior Lecturer in the Department of Information Science, University of South Africa, Pretoria

Unfortunately, in various public institutions such as archival repositories and governmental bodies, vast amounts of digital records are stored in an unstable digital environment (Ngoepe 2017). In some instances, ARM systems are left open to attacks by security threats due to a lack of implementable robust security features. Unprotected or vulnerable ARM systems tend to allow malicious people to access digital records and place classified and confidential records at risk of being tampered with (Ngoepe 2017). This is because due to resource deficiency such as insufficient budgets, many government institutions around the world tend to implement very little security on their systems and thus these systems are exposed to and targeted by cybercriminals (Katuu 2012). As such, these sophisticated criminals continue to exploit vulnerable records management systems containing valuable digital records for their own benefit.

2 Problem statement

Despite the growing importance of digital curation of archives, many governmental bodies suffer from lack of infrastructure and reliable technology to ensure security for these digital materials. This is also the case in South Africa, where public institutions end up storing valuable digital materials in insecure storage devices (Ngoepe 2017; Katuu 2012). As such, security of digital archives remains a significant concern. Security or lack thereof, tends to lead loss, theft, and manipulation of significant materials (Katuu 2012). This also coupled with issues related to interoperability of systems, especially when organisations require to move digital archives from old storage devices to new one. The infrastructure and technology tend to be incompatible, resulting in valuable records being permanently locked in those ARM systems. Therefore, without robust security measures, staff, hackers, viruses and malwares tend to compromise these systems. In turn, they jeopardise the authenticity, integrity, confidentiality and reliability of digital records in governmental systems. Such acts also threaten to violate violating legislative frameworks such as the Protection of Personal Information Act (POPIA) in South Africa (Lubua, Semlambo & Mkude 2022).

The implementation of FOSS for digital curation of archives can provide more secure, dependable, compatible, interoperable, and less costly technology and infrastructure. According to Karume and Mbugua (2012), this is because FOSS products provide users with the option of a detailed review of the source code, giving users the ability to fix problems themselves without having to wait for the vendor. The developers to FOSS can be able to add or modify additional features to the program's source code to make it more secure from potential threads. The developers or contributors of FOSS can work without any restrictions, and this allows them to rectify errors that might have been missed by the original developers or publishers (BBC 2022). Moreover, the FOS community prioritise and ensures the constant review and monitoring of their software's is never a one-off activity, but rather an ongoing process that ensures vigilance, quick responsiveness, and adaptability (Bwalya, Akakandelwa & Dobreva-McPherson 2019). This also means that breaches of security can be detected much easier due to the software being managed by a community of developers and programmers. Open-source software presents a cost-effective and flexible solution for managing digital archives. In this way FOSS provide a strategic way of dealing with threats posed by file format obsolescence, system viruses and cybercriminals.

FOSS is also deemed as being safer than proprietary software because it allows the flexibility of collaborating with other software developers in a bid to produce robust security measures that are difficult to bridge. According to Techopedia (2012), Linux (a FOSS operating system) is perceived to be the leading technology because it is seen as more dependable and safer than Microsoft Windows (a proprietary operating system). Therefore, the attainment of the Linux operating system (for example) makes the concept of FOSS attractive to various organisations that deal with information and communication technology activities. In this way, FOSS provided more security to records stored in digital systems, to ensure that records are kept in their original format as created or received and securely against possible alteration.

3 Purpose and objectives of the study

The purpose of this study was to explore security measures for digital archives curated through open-source software in South Africa, with the view of proposing strategies to enhance utilisation of free open-source software. The specific objectives were to:

- Assess the policy and legislative frameworks relating to security for digital archives curated through open-source software.
- Evaluate open-source software security measures for digital curation of archives in South Africa.
- Propose strategies for utilising FOSS solutions to enhance security for digital curation of archives.

4 Review of the literature

The section presents the literature review

4.1 Regulating frameworks relating to security for digital curation of archives

In South Africa, like many other countries, the security for digital archives has become a paramount concern. This has increased efforts to develop robust regulating framework that include policies, legislations, and standards (Choudhury et al. 2020). AS such, multifaceted approaches are sought aimed to safeguarding the confidentiality, integrity, and accessibility of digital records, ensuring their preservation for future generations. Hence, proper implementation of security measures should be regulated by legal framework (Chen, Fu, Sun, Bilgihan & Okumus 2019). Such legal framework aid in equipping relevant staff with legitimate access rights to digital system, as well as the power to act in accordance to stipulated guidelines. This may also ensure that unauthorised staff can easily gain access to the system for the purposes of committing fraud, altering records as well as bridging IT infrastructure (Chen, Fu, Sun, Bilgihan & Okumus 2019).

In South Africa, the government has enacted a number of laws that ensure the security of digital archives. These include the Protection of Personal Information Act of 2013 (POPI Act), Promotion of Access to Information Act of 2000 (PAIA), National Health Act of 2003 (NH Act), Promotion of Administrative Justice Act of 2000 (PAJA), Electronic Communication and Transaction Act of 2002 (ECT Act), National Archives of South Africa Act of 1996, and the Constitution of the Republic of South Africa (Act No. 108 of 1996). The NARSSA Act, which is the supreme records and archival regulatory legislation, requires all government agencies to manage, retain, and make all forms of records available in a variety of media. These records need to be managed in accordance with relevant archival legislative guidelines and subsequent policies. South Africa's legislative and regulatory system has a pronounced impact on how records are managed in the various government structures or entities. Thus, it is the responsibility of public sector organisations to keep or preserve records in such a way that their integrity is maintained, and they remain traceable and accessible when they are needed. This would allow organisations to account for their past activities and establish whether they comply with the relevant policies or guidelines governing records management (NARSSA 2006).

4.1 Policies relating to security for digital curation of archives

When it comes to policies, Wright (2012) implies that they should be implemented to guide the curation of archives processes in archival institutions. Such policies should include content development and management for a digitisation and preservation policy; collection of disaster plans; statements on open access to digital resources, storage, security, and intellectual property; and reference to copyright and metadata policies (Ndenje-Sichalwe 2010). Implementing of organisation policies to ensure vigorous security controls for digital records systems cannot be over-emphasised. Such a policy should address key activities and guidelines relating to ensuring that technology and infrastructure used to store digital records provide better security, backup, interoperability, and preservation of digital records. Such a policy should also ensure that private and highly confidential records may only be access by authorised staff.

The are various polices that are used in South Africa in a bid to grapples with the complexities of digital preservation. These policies differ from organisation to organisation, and they depend on the type of implemented software for digital curation of archives. Some of the common policies in the sphere of digital curation of archives include the Minimum Information Security Standards (MISS), Records Management Policy Manual, IT Disaster Recovery plan policy and the National Cybersecurity Policy Framework, to mention just a few. They are important in guiding public institutions toward a resilient records management security, continued access, and cybersecurity posture. Alongside these, organisational policies specific to digital preservation and data protection impact assessments contribute to a comprehensive security tool.

4.3 Standards relating to security for digital curation of archives

As alluded by Chuma and Ngoepe (2021) governmental bodies are required to establish the standards that protect sensitive information pertaining their systems and records. Digital records management systems in particular, required to adhere to universal approved principles, guidelines, and standards (Chuma & Ngoepe 2021). The principles, guidelines, and standards help in ensuring authenticity, reliability, and accuracy of records are at the root of records and archives management. The main aim is to ensure continuous access and retrieval of digital records.

Apart from ensuring security of digital archives, universal accepted standards also provide basis to ensure interoperability of digital records systems. This is important when governmental bodies need to transfer or migrate digital records to new storage mediums, across one another, and to preservation agencies when the need arise. Standards, especially those for interoperability of systems, are vital for enabling safe and secure exchange and sharing of information between different systems (Marutha 2019). This may include international standards, such as ISO/IEC 27001 for information security management and ISO 16363 for trustworthy digital repositories, alignment to national archives and records service of South Africa guidelines, as they provide benchmarks for organisations engaged in digital curation of archives.

OpenDocument Format (ODF), a free and open-source software file format, stems from the open XML-based OpenOffice.org specification and was approved by ISO as a standard in 2006 (Chen, Fu, Sun, Bilgihan & Okumus 2019).

In terms of guaranteed long-term availability, international standards bodies rendered ODF the safest file format (McHugh 2021). Moreover, FOSS involves representatives from different constituencies being involved in creating the standard, helping to ensure that it balances the needs of a wide variety of users and offer high level of interoperability even with software's of other kinds.

4.4 Security measures for digital curation of archives in South Africa

Robust security to ensure integrity and swift transfer of records from creating agencies to archival institutions can never be overemphasised. The security of digital archives is essential in ensuring that such material remains accessible, usable, transferable, and can be used over long periods of time (Ngwenya & Ngoepe 2022). The records lifecycle model emphasises that the main reason for digital curation of archive, is to safeguard continuous access to these records whenever a need arises (Lin 2015). However, ensuring security for large and ever-expanding collections of digital materials has proven to be a mammoth task for archival institutions around the world (Corrado & Moulaison 2014). Digital records are fragile materials that must be handled in a manner that ensures they are secure.

Unfortunately, in various public institutions, such as archival repositories and governmental bodies, vast amounts of digital records are stored in an unstable digital environment (Ngoepe 2017). In some instances, ARM systems are left to be attacked by security threads due to a lack of implementable, robust security features. Unprotected or vulnerable ARM systems tend to allow malicious people to access digital as well as place classified and confidential records at risk of being tempered with (Ngwenya & Ngoepe 2022). This is because many government institutions around the world tend to implement very little security on their systems and thus become exposed to and are targeted by cybercriminals owing to resource deficiency such as insufficient budgets (McHugh 2021). As such, these sophisticated criminals continue to exploit vulnerable records management systems that contain valuable digital records for their own benefits.

FOSS can provide more secure, dependable, and less costly technology when it comes to security. According to Karume and Mbugua (2012), this is because FOSS products provide users with the option of a detailed review of the source code, giving users the ability to fix problems themselves without having to wait for the vendor. On the other hand, proprietary products that are often rented tend to be packed with security vulnerabilities (Buffett 2014). Hence, according to Techopedia (2012), Linux (a FOSS operating system) is perceived to be the leading technology because it is seen as more dependable and safer than Microsoft Windows (a proprietary operating system). Therefore, the attainment of the Linux operating system (for example) makes the concept of FOSS attractive to various organisations that deal with information and communication technology activities.

Gangadharan (2017) argues that FOSS implementation can provide solution related to safeguarding of digital materials. The author reiterates that FOSS may grant governmental bodies a higher degree of vendor independence, security, and system interoperability. In the same vein, Ngoepe (2015) as well as Oreku and Mtenzi (2013) point out that the FOSS-based development model reduces costs and risks associated with security, while improving productivity and quality. This means that the implementation of FOSS for digital curation of archives in South Africa may provide governmental bodies with quality and secure technology at a lower cost than proprietary software. This may be helpful provided that institutions such as governmental bodies, including the national archives of South Africa, which is consistently lamented by scholars for lacking the necessary technological infrastructure resources, that may also ensure safe and secure storage of such materials.

Security to ensure systematic and seamless transfer of digital records, particularly in digital systems, ensures that records are kept in their original format as created or received and securely against possible alteration. The record lifecycle models point out that the access, use, and reuse of digital records heavily depend on the safety of the digital systems in which they are stored (Lin 2015). In this way, the safety of systems enables the continual utilisation, access, and distribution of digital records, which are the fundamental requirements of the records lifecycle model. This thus calls for the implementation of robust actions and techniques to mitigate possible threads that may hamper the transfer of digital records (Ngwenya & Ngoepe 2022).

Reliability of digital records is concerned with establishing the dependability of a record as a statement of fact by examining the completeness of the record's form and the amount of control exercised in the process of its creation (Chen, Fu, Sun, Bilgihan & Okumus 2019). A record is deemed reliable when it can be treated as a fact, that is, as the entity of which it is evidence. The authenticity and reliability of digital records in a records management system convey the trustworthiness of records. This means that digital records kept in the system contain accurate statements of facts and a genuine manifestation of those facts. As asserted by Ngwenya and Ngoepe (2022), some security measures that should be guarded against include the following: file format and technology obsolescence, human errors by both authorised and unauthorised staff, and cybersecurity.

5 Methodology

This qualitative study triangulated interviews with document analyses to explore the ingestion of digital records into archival custody through free open-source software in South Africa. Interview data were collected from records managers and chief information officers from purposively selected public entities that have implemented electronic content management, as well as archivists and IT officials from the NARSSA and State Information Technology Agency (SITA), responsible for archival system implementation. The NARSSA and SITA were contacted to provide the names of national government departments that have implemented systems for digital records management and preservation in South Africa. These two organisations usually work hand in hand with governmental bodies that manage digital records in South Africa. Directors and, in some instances, chief directors of each department were contacted to acquire permission to conduct the study in the institution.

The key measure based on which the population of this study was selected was that they worked relatively close to digital records management and preservation in their respective organisations. For instance, archivists and records managers are tasked with performing a strategic and executive role on records, including digital records, as part of their key duties. At times, they are accountable for the digital curation of archives. As such, the decision to choose archivists and records managers in this study was because they were able to share their knowledge and expertise on the software implemented for the digital curation of archives and, ultimately, the preservation of such records. As reflected in Table 1, semi-structured interviews were conducted with 13 participants, including records managers, archivists, and IT specialists. Data were analysed and presented thematically with the use of word clouds, figures, tables, and verbatim quotations, as in line with the objectives of the study.

6 Findings of the study

The following are the findings of the study conducted in national government departments as well as NARSSA. Interviews and document analysis were utilised to collect data with Archives and Records managers as well as ICT personnel. To ensure anonymity and confidentiality of participants, ARMP- code was assigned for archives and records managers, whereas ICTP- code was used for ICT personnel. Data was presented through table, word clouds and verbatim quotations. Data was analysed thematically in line with research objectives. Table 1 indicate the themes, subthemes, and category of security of digital curation of archives:

Table 1: Themes, subthemes and categories of security of digital curation of archives

Themes	Categories	Sub-categories
Theme 1: FOSS policy, standards, and legislative framework for security of digital curation of archives	1.1 Policy used for security of digital curation of archives	• IT Disaster Recovery plan policy • Institutional policy on records management • Minimum Information Security Standards (MISS), • Records Management Policy Manual • Utilisation of SA FOSS policy
	1.2 Legislative framework for security of digital curation of archives	• The Public Service Corporate Governance of Information and Communication Technology Policy Framework (CGICTPF) • National Archives and Records Service Act (No. 43 of 1996) • Promotion of Administrative Justice Act (No. 3 of 2000) • Electronic Communication and Transactions Act (No. 25 of 2002) • Promotion of Access to Information Act (No. 2 of 2000) • Protection of Personal Information Act, (No.4 of 2013).
	1.3 Standards for security of digital curation of archives	• ISO/SANS15489 records management • ISO 31010: 2009 Risk Management- principle and guidelines

		• Minimum Security Standards (MSS) • Not aware of the existing standards currently used.
Theme 2: Security measures in the digital curation of using FOSS.	• Cyber security threats	• System virus • Hacking of system • Firewall
	User controls	• Authentication measures • Passwords and usernames • Privacy issues • Reskilling

6.1 Policies, standards, and legislative frameworks for security of digital curation of archives

The first objective of the current study, it was important to assess and analyse policy, standards, and legal framework used for security for digital curation of archives by both national government departments and NARSSA. This was achieved through document analysis as well as through the interviews with participants of the study. The participants who took part under this theme were asked to elaborate on the policies, standards and legislative framework that are currently used for digital curation of archives. Figure 1.1 shows the sub-themes through the cloud words that emerged from the findings obtained in the first research objective.

Figure 1: Themes emerged from the findings about policies and legislative framework

As advocated by (Marutha 2019) policies for security of digital curation of archives are developed in order to provide direction on how records will be created, shared, utilised, transferred, stored, and ultimately preserved. Hence, it is imperative that each unit of the organisation formulate or adopt records management policies to appropriately manage and preserve important records. Participants of the study provided various perspectives when asked to elaborate on the policies used by their organisations in relation to security of digital curation of archives. The following policies, namely, Minimum Information Security Standards policy, IT Disaster Recovery plan policy, Records Management Policy Manual, as well as various policies that were devised by individual organisations in a bid to guide the digital curation of their archives (Marutha 2019). It was also established that even though some of the participating organisations did implement FOSS solutions for digital curation of archives, their records management policy statement was not addressing or based on open-source software.

The study was also keen to establish legislative frameworks that are currently being utilised for security of digital curation of archives. The study relied on participants responses through interviews as well as document analysis to gather information pertaining legislative frameworks guiding digital curation of archives in national government departments and NARSSA. It was noted that majority of these organisations that formed part of the study, were mostly using similar legislative frameworks. The responses indicated that the commonly used legislative framework include:

- The Public Service Corporate Governance of Information and Communication Technology Policy Framework (CGICTPF)
- National Archives and Records Service Act (No. 43 of 1996)
- Promotion of Administrative Justice Act (No. 3 of 2000)
- Electronic Communication and Transactions Act (No. 25 of 2002)
- Promotion of Access to Information Act (No. 2 of 2000)
- Protection of Personal Information Act, (No.4 of 2013)

These findings were consistent with the legislations that are provided on NARSSA website, listed as the most used in terms of records management including the security of records. Moreover, participants of the current study have also shown that their respective organisations, indeed do follow the above-stated legislation in digital curation of archives. Lastly on the first objective, was to establish some of the best practices and standards that are currently used for digital curation of archives in South Africa. Participants of the study have indicated that their respective organisations are currently following the globally accepted standards for records management that include ISO/SANS15489 records management, ISO 31010: 2009 Risk Management- principle and guidelines, Minimum Security Standards (MSS). The participants of the study also allude that using an international standard allows for end users to find digital curation of archives that are relevant to their needs.

6.2 Security measures for digital curation of public archives

This objective sought to identify security concerns and measures put in place to counter such problems in the digital curation of archives. Literature points that, due to lack of sufficient budget to purchase sophisticated systems, hardware, software, and firewalls, security of archives in most government departments is compromised. This is also coupled by the problem of not being able to attract skilled, experienced, and knowledgeable IT personnel in government departments to ensure system security. Figure 1 depicts a word cloud of security concerns experienced by participants in the digital curation of archives throughout their respective organisations. In turn, participants indicated that they sometimes felt uncertain about the levels of security in records management system, owing to the stated issues.

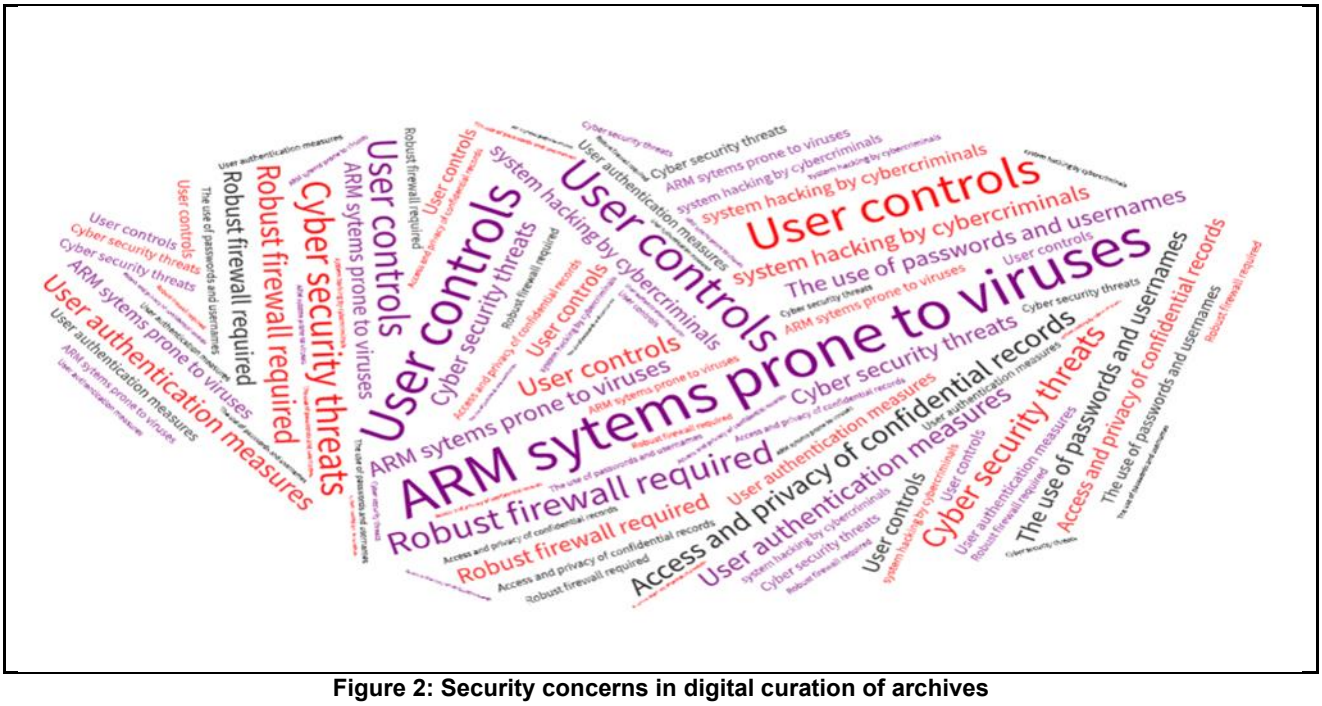

Figure 2: Security concerns in digital curation of archives

The participants agree that cybercriminals tend to target public sector records management systems due to their vulnerability of being easy to access. This is due to popular belief that many government departments still operate with outdated software and hardware which are easy to bypass. However, the common agreement by participants is that security of records management systems is currently prioritised to curb easy access, retrieval, theft, manipulation, altering and tampering with the archives by both staff and possible unauthorised users. The participants of the study have also concurred that their organisations are yet to be confronted by any serious security thread. These sentiments were shared by all participants regardless of the type of software implemented for digital curation of archives. Participants mentioned that their departments ensured the safety of stored information by implementing various measures to mitigate the security of records.

For instance, ARMP-2 mentioned that their current implemented security measures are able to fend off risk of ARM system security concerns. The participant viewed this as a huge security and stated that: ARMP-2 mentioned the following:

> *"So far there has not been issues with open source in our department. No major incident just yet. However, in 2018, there was a reported hacking of our website, but the records management database was never reached. The issue was quickly dealt with by our ICT team and until now, I have not really experienced any real danger of security concerns".*

These sentiments were also support by ARMP-1, who indicated that their current ARM system is yet to witness any threads, despite losing key ICT staff members:

> *"I reckon you that the current system is safe for our digital records. However, we have lost two crucial staff members and think, the department should support us with more skilled ICT personnel who can be able to implement security measures such as, end-point security, firewall, and VPN Service to access to the records management system utilising open-source."*

6.3 Strategies to enhance security for digital curation of archives through FOSS

The following are the recommended strategies to enhance security for digital curation of archives through FOSS in line with the findings of the study:

The study discovered that the implementation of FOSS policy, legislations, and standards for security of digital curation of archives by national government departments is currently at low to no existence in terms of utilisation rate. The situation seems to not to improve despite FOSS utilisation in South Africa being supported by policy endorsed by Cabinet of South Africa. Therefore, the study recommends amendments of legislations, policies and standards relating to security of digital curation of archives in governmental bodies to include FOSS. This in turn will be beneficial and increase the implementation rate of FOSS. Moreover, it is important that South African FOSS policy for governmental use be made compulsory rather than a mere recommended choice in public sector.

FOSS security for digital curation of archives seems to be more advantageous as compared to other software products. Some of its benefits in security of digital curation of archives include being a key role player in IT development industry, ability to alter, change and improve the software to meet the user's needs, affordability, and no licence fees to name just a few. In this sense, user control measures can be made robust, cybersecurity, firewall breaches, and viruses can be detected as soon as possible, most importantly, access, retrieval, privacy, and confidentiality may be achieved. Moreover, rigorous marketing, promotion and raising awareness of FOSS products for security of digital archives, especially by governmental bodies that have already implemented the software, can go a long way in accelerating its utilisation rate. By so doing, FOSS solutions may assist governmental bodies to safeguard the integrity as well as completeness of their digital archives.

7 Conclusion

In South Africa, like many countries, security of digital curation of archives of governmental bodies, is conducted in line with legislative framework. However, when it comes to the implementation and the use of FOSS for digital curation of archives, the legislative framework pertaining to security of records management seems to be silent in providing guidelines for its utilisation. This continues to happen even when the cabinet of South Africa, have endorsed and drafted policy for FOSS utilisation across governmental bodies in over two decades. This study explores the security for digital curation of archives through FOSS in South Africa and provides strategies that may be followed to enhance security for digital curation of archives through FOSS. The security of digital curation of public archives is a serious concern for governmental bodies in a bid to safeguards digital archives. This is also the case for NARSA which is mandated to preserve significant, historical, and sensitive digital archives. FOSS has the capability of leveraging security for digital curation of archives these governmental bodies. As argued by the study, the first step should be the amendment and subsequent inclusion of FOSS

in records management legislations, policies, and standards. As such, FOSS presents an opportunity not to be missed by governmental bodies in South Africa in a bid to strengthen the security of digital archives.

References

BBC.2022. Ethical, legal, and environmental impacts of digital technology – OCR. [Online] https://www.bbc.co.uk/bitesize/guides/zhx26yc/revision/9#:~:text=Open%20source%20software%20can%20be,and%20only%20available%20under%20licence (17 November 2023).

Buffett, B. 2014. *How IT can contribute to changing organizational culture: Factors influencing open-source software adoption in public sector national and international statistical organizations*. Meeting on the Management of Statistical Information Systems (MSIS 2014): (Dublin, Ireland and Manila, Philippines 14-16 April 2014).

Bwalya T., Akakandelwa A. and Dobreva-McPherson M. 2019. Adoption and use of free and open-source software (FOSS) globally: An overview and analysis of selected countries. [Online] https://www.researchgate.net/publication/337318071Adoption_and_Use_of_Free_and_Open_Source_Software_FOSS_Globally_An_Overview_and_Analysis_of_Selected_Countries (16 October 2025).

Cheng, X., Fu, S., Sun, J., Bilgihan, A. and Okumus, F. 2019. An investigation on online reviews in sharing economy driven hospitality platforms: A viewpoint of trust. *Tourism Management,* 71: 366-377. https://doi.org/10.1016/j.tourman.2018.10.020

Chuma K.G. and Ngoepe M. 2021. 36. Security of electronic personal health information in a public hospital in South Africa. *Information Security Journal: A Global Perspective,* 31(2): 179-195. DOI: 10.1080/19393555.2021.1893410

Corrado, E.M. and Moulaison, H.L. 2014. *Digital preservation for libraries, archives, and museums*. Lanham, MD: Rowman and Littlefield Publishers.

Digital Preservation Coalition. 2022. Digital preservation handbook. (Online) https://www.dpconline.org/handbook. (03 September 2023).

Gangadharan, G.R. 2017. Open-source solutions for cloud computing. *Computer,* 50(1): 66-70.

Gupta, D. and Surbhi, G. 2018. Adopting free and open-source software (FOSS) in education: *I-manager's Journal of Educational Technology*. [Online] https://eric.ed.gov/?id=EJ1179515. (22 January 2025).

ISO 15489-1. 2016. Information and documentation – Records management – Part 1: [Online] concepts and principles. *International Standards Organisation for Standardization.* https://www.iso.org/standard/62542.html (15 November 2025).

Karume, S. and Mbugua, S. 2012. Trends in adoption of open-source software in Africa: Journal of Emerging Trends in Computing and Information Sciences. [Online] http://www.cisjournal.org/journalofcomputing/archive/vol3no11/vol3no11_10.pdf (24 January 2025).

Katuu, S. 2012.Enterprise content management (ECM) implementation in South Africa. *Records Management Journal,* 22(1), 37-56.

Katuu, S. 2015. Managing records in South Africa's public sector – a review of literature. *Journal of the South African Society of Archivists* (48), 1-13.

Lin, C.Y. 2015. Toward a holistic model for the management of documents, records, and Archives. *Archival Issues,* 37(1): 21-47.

Marutha, N.S. 2019. Archives and records management legislations and standards. Tutorial Letter 501/3/2019. Pretoria: University of South Africa.

McHugh, R. (2021), *Different types of security in records management*. [Online] https://www.recordnations.com/2019/01/different-types-security-in-records-management/ (12 August 2025).

Ngoepe, M. 2015. Deployment of open-source electronic content management software in national government departments in South Africa. *Journal of Science and Technology Policy Management*, 6(3): 190-205. https://doi.org/10.1108/JSTPM-05-2014-0021

Ngoepe, M. 2017. Archival orthodoxy of post-custodial realities of digital records in South Africa. *Archives & Manuscript,* 45(1): 31-44. https://doi.org/10.1080/01576895.2016.1277361

Ngoepe, M. and Saurombe, A. 2016. Provisions for managing and preserving records created in networked environments in the archival legislative frameworks of selected member states of the Southern African Development Community. *Archives and Manuscript,* 44(1): 24-41. https://doi.org/10.1080/01576895.2015.1136225

Ngoepe, M. and Kenosi, L. 2022. Confronting Jenkinson's canon: Reimagining the 'destruction and selection of modern archives' through the Auditor-General of South Africa's financial audit trail. *Archives and Records*, 43(2): 166-176. doi:10.1080/23257962.2022.2048639

Ngwenya, M. and Ngoepe, M. 2022. Data trust in Consumer Internet of Things assemblages in the mobile and fixed telecommunication operators in South Africa. *South African Journal of Information Management*, 24(1): 1-9. [Online] http://dx.doi.org/10.4102/sajim.v24i1.1426 (10 November 2024).

Oreku, G. S., & Mtenzi, F. J. (2013). Adoption and diffusion of open-source software in Tanzania: A way forward. In 2013 IST-Africa Conference and Exhibition, IST-Africa 2013 Article 6701748 (2013 IST-Africa Conference and Exhibition, IST-Africa 2013). IEEE Computer Society.

Shekgola, M., Maluleka, J., and Rodrigues, A. 2021. Factors influencing the adoption of free and open-source software for electronic records management by municipalities in Gauteng Province, South Africa. *Journal of the South African Society of Archivists*, 54: 43–54. https://doi.org/10.4314/jsasa.v54i1.4

South African Government. 1996. *National Archives and Records Services of South Africa Act 43 of 1996*. [Online]: http://www.kznworks.gov.za/publications/ policy/NationalArchivesActand Regulations.pdf (20 March 2025).

South African Government. 1996. *National Archives Act, No. 43 of 1996*. Pretoria: Government Printer.

South African Government. 2000. *Promotion of Access to Information Act, No. 2 of 2000.* Pretoria: Government Printer.

South African Government. 2002a. *Electronic Communications and Transactions Act, No. 25 of 2002*. Pretoria: Government Printer.

South African Government. 2002b. *Regulation of Interception of Communication and Provision of Communication-related Information Act, No. 70 of 2002*. Pretoria: Government Printer.

South Africa. 2013. *Protection of Personal Information Act, No. 4 of 2013*. Pretoria: Government Printer.

Techopedia. 2012. *Open Source: Too Good to Be True*? [Online] https://www.techopedia.com/2/28968/software/open-source-is-it-too-good-to-be-true (25 October 2025).