ISS INSTITUTE FOR SECURITY STUDIES

South African
CRIME QUARTERLY
No. 74 | 2025

Electronic records management and provision of justice

Keeping e-dockets secure in Limpopo police stations

Alex Lesiba Legodi and Maoka Andries Dikotla[1]

legodal@unisa.ac.za
edikotm1@unisa.ac.za

https://doi.org/10.17159/sacq.n74.19281

In the criminal justice system, effective records management is essential for justice delivery and the protection of human rights. This study investigates the security and backup measures used to safeguard electronic dockets in the South African Police Service (SAPS), focusing on selected stations in Limpopo Province. The SAPS adopted the e-docket system to address persistent problems with manual docket management, including loss, tampering, and delays. Using an exploratory survey design and quantitative approach, data was collected through a structured questionnaire presented to purposively selected police officers. The findings reveal that access to the e-docket system is primarily secured through passwords, making it vulnerable to unauthorised access. Moreover, most stations rely on manual backup systems without off-site storage, leaving electronic records exposed in the event of system failure or disaster. These weaknesses threaten the reliability and integrity of case records, with serious implications for justice administration.

Introduction

Digital records are a reality for most public sector institutions.[2] The proper administration of legal records is central to the delivery of justice and the protection of citizens' rights. Therefore, the security and protection of records in the

custody of the South African Police Service (SAPS) cannot be overemphasised, as records can either make or break justice service delivery and may be necessary for the protection of other fundamental human rights. Dockets are recognised as critical components of the criminal justice system and are essential to its effective operation.[3]

A docket is an official document in which a record of a reported crime and the related investigation is kept.[4] Police dockets serve as comprehensive case files that document all pertinent details, including the incident, victim and witness testimonies, law enforcement actions, and the progress of the case through the justice process.[5] A standard police docket is divided into three parts: Section A includes witness statements, expert analyses, and documentary proof; Section B holds internal communications such as reports and memoranda; and Section C contains the investigation diary.[6] Although there are other police records, such as occurrence books and cell registers, dockets are the most comprehensive and vital case records, necessary for court processes and judicial decision-making.[7]

Manual docket systems have long been associated with inefficiencies. They have often been reported missing or delayed, preventing courts from proceeding with prosecutions.[8] These administrative failures delay or deny justice and undermine the image of SAPS and the credibility of the broader criminal justice system. Reliable and authentic records are essential to the delivery of justice to both victims and the accused, and should be protected from both damage and unauthorised access. While measures such as access controls and physical security are commonly used for managing records, SAPS, like many organisations, has struggled to implement them consistently.[9] For years, it has been plagued by docket mismanagement, resulting in miscarriages of justice.[10]

To address these problems, SAPS introduced the Integrated Case Docket Management System (ICDMS), also known as the e-docket system.[11] This system provides an integrated method of monitoring police dockets and aims to correct the inefficiencies of the manual system. Its purpose is to support SAPS in fulfilling its constitutional mandate of enforcing the law and bringing offenders to justice, as outlined in Sections 205 to 208 of Chapter 11 of the Constitution of the Republic of South Africa, 1996.[12]

Despite the potential benefits of electronic records systems, the literature identifies risks such as privacy breaches, identity theft, and data loss, which can negatively affect productivity and justice delivery.[13] The e-docket system is not immune to such threats. It remains vulnerable to risks, including loadshedding and cybersecurity breaches.[14] Once security is breached, records may be altered or deleted, undermining their reliability. When such events destroy records altogether, the result is an information disaster. It may lead to failed prosecutions and, in some cases, civil claims against SAPS for violating the personal information of victims.[15]

In today's high risk environment, a strong security, backup and recovery strategy is essential. Organisations that succeed in the long term typically invest in proactive disaster recovery plans.[16] Many forward-looking institutions have adopted cloud computing, which allows data to be stored across multiple locations. Although it entails some cost, cloud storage enables unlimited capacity and improved access.[17] Governments worldwide are increasingly integrating cloud computing into their daily operations to reduce costs and make more efficient use of resources.[18] For example, many public institutions in Kenya

have transitioned to cloud-based platforms for records management, leveraging them as efficient and economical technological solutions.[19] Similarly, Ugandan commercial banks have embraced cloud-computing systems, enabling virtual management and enhancement of their data storage capabilities.[20] These developments have improved service speed and reliability. With regard to the SAPS, cloud storage should, among others, allow prosecutors to retrieve dockets remotely, without needing police officers to deliver them in person.

A well-functioning records management system ensures that records are safe, accurate and easy to access, which in turn safeguards justice for citizens, as well as ensuring accountability and transparency.[21] However, without strong system security and institutional capacity, the intended benefits of e-government systems may be compromised.[22] Electronic systems are highly susceptible to malfunctions and hacking, and they need frequent software upgrades.[23] Records management that is implemented improperly culminates in poor service delivery, because government records are an important element of a well-functioning administration and a way for citizens to hold governments to account.[24] If the implemented computer systems do not facilitate access to reliable and authentic records, they will likely be a liability rather than an asset.[25] Depending on how an electronic records management system is implemented, it can either support or compromise the delivery of justice.[26]

Good records management is an indispensable resource for fighting crime.[27] However, despite their importance, the security and backup measures of the SAPS e-docket system have not yet been systematically studied. In this study, the researchers explored the measures that have been put in place to ensure the integrity of electronic records on the e-docket system in six police stations in Limpopo Province. The specific objectives were to:

- Identify security measures implemented to regulate access to electronic records on the e-docket system.
- Determine the nature of the backup and recovery plan for records on the e-docket system.
- Propose a framework that may be adopted for the improvement of security measures in SAPS police stations in Limpopo Province.

The e-docket as an electronic record management system

The e-docket is an electronic system introduced by the SAPS for storing criminal dockets. An electronic records system refers to all components of an electronic information system, namely electronic media and all connected items, such as source documents, output information, software applications, programmes and metadata.[28] It permits the monitoring of all the operations or transactions through which the record has passed, and its metadata, from the moment of its creation and capture within the system.[29] Electronic systems introduce transparency and efficiency in managing records by bringing different functions into a single system, and provide the means to track and monitor records.[30] The implementation of ICT systems has broadened the field of records management and made it possible to manage records electronically and remotely. Electronic records management involves managing both records originally created in digital form, and those converted from paper formats.[31]

Electronic records systems are typically categorised into Electronic Records Management Systems (ERMS), Electronic Document Management Systems (EDMS), and Electronic Records and Document Management Systems (ERDMS), which combine both

functionalities. The e-docket system used by the SAPS is best understood as an ERDMS, although in practice it is a hybrid electronic records management system, as it is still being phased in and therefore also makes use of a manual records management system.[32] Dockets are created manually and are later scanned to convert into an electronic format on the e-docket system, either during the progression of the case or, in some instances, after the completion of a case. In some such cases, dockets have been lost or compromised in the conversion process.[33]

The e-docket system generates e-dockets, which are predominantly used by detectives,[34] but serves the police and the entire justice system and facilitates the sharing of information about criminal cases among officers and detectives, from the beginning of a case to the end.[35] The e-docket system is intended to reduce maladministration, corruption and documentation loss while improving service quality, information access, accuracy and collaboration among officers.[36] The adoption of the e-docket system is also intended to make files auditable and traceable, and almost impossible to delete within the system.[37]

Security and access control

Electronic records management systems require strong security. The three pillars of securing protected information are administrative safeguards, physical safeguards and technical safeguards, with safeguarding techniques ranging from the location of computers to the use of firewall software to protect digital records.[38] Appropriate access controls must be maintained for as long as the organisation needs the records.[39] Efficient management of e-records is critical to ensure the protection of vital records,[40] and a well-organised records management system should trace the movement of current records throughout the organisation to identify any intentional or accidental unauthorised actions.[41]

Even with such security measures in place, records on digital platforms are susceptible to more diverse and flexible risks than those in paper form.[42] The issue of access control to records on the e-docket system has become even more critical after it was revealed that a significant number of criminal records were negatively affected by e-docket system malfunctions.[43] The insecurity of records is largely a result of mismanagement, "where records may be accessible, but the information recorded is incomplete, concealed, altered, amended, and/or added".[44]

System backup and recovery

All institutions are at risk of experiencing a disaster, be it natural or man-made. Hence, security measures need to include backup and other copies of stored information, as their integrity is of importance in circumstances where they have been used as replacements for live data.[45] System backup refers to information that is stored elsewhere to be utilised in times of system failure or data loss,[46] while a disaster recovery plan refers to the measures put in place ahead of time on how to restore operations in the case of disaster.[47]

The purpose of a backup and disaster recovery procedure is to reconstruct authentic and reliable records, making it essential that backup data includes associated metadata and audit trails of all records so that the authenticity of recovered records is not compromised.[48] However, many public sector institutions are found wanting when it comes to system backup and recovery plans. The absence of a disaster preparedness plan is one of the impediments to proper records management in many public sector institutions, thus exposing an organisation to memory loss should a disaster strike.[49] Without a disaster recovery plan, a vital

records schedule and a retention schedule, an "organisation is sitting on an 'information ticking time bomb' that could have dire consequences, such as loss of vital memory, should the bomb not be diffused".[50]

Additionally, "the threats of unstable media, of ever-changing software and hardware and of data security place an organisation's electronic memory at risk".[51] Backup copies of current records, kept off-site, ensure against disaster. Backup and disaster recovery plans and strategies allow a governmental body such as the SAPS to rebuild its electronic information and to continue operations in the event of significant network failure or other disasters.[52] A data backup and recovery plan in line with best practices entails a definition of the specific data to be backed up, the type(s) of backup to be used, the frequency and time of data backup, responsibility for data backup, the storage site(s) for the backups, and the storage media to be used.[53]

A system backup and recovery plan is crucial if the e-docket system is to have its intended benefits in the SAPS and the criminal justice system. The impact of the lack of backup on the management of court records was highlighted when, during load-shedding, backup electricity supply was not available, making it difficult to access electronic records, and thus causing delays to the justice delivery process.[54]

Methodology

The study adopted an exploratory survey research design to investigate the security and backup measures put in place to ensure the integrity of electronic records on the e-docket system for effective administration of justice. The collection of data for this study took place in 2020. Due to resource constraints, the study focused on two of the 13 clusters in Limpopo Province, namely Mankweng and Lebowakgomo, as they were easily accessible to the researchers. Permission to conduct this study was obtained from the SAPS national office before a closed-ended questionnaire was distributed to police officers in a face-to-face manner. Purposive sampling was used to select 100 police officers with knowledge of the e-docket system and who work with the e-docket system on a daily basis. To minimise bias, the questionnaire was pre-screened for possible leading questions, and to ensure anonymity, personal data of the participants was not collected. Of the 100 questionnaires that were distributed, 65 were returned, thus yielding a 65% response rate. This response rate is considered good enough to draw valid conclusions and recommendations.[55] Quantitative data analysis was done through descriptive statistics using the IBM Statistical Package for the Social Sciences (SPSS V26 for Windows).

Limitations and generalisability

The findings of this study, which employed an exploratory survey design, cannot be generalised to other police stations in other provinces. The intention of this exploratory research study was to gain insight into whether the implementation of the e-docket system enhanced or compromised the administration of justice in selected police stations in Limpopo Province. Consequently, because of the focus on a select few police stations, the conclusions of this study cannot be applied to all police situations; however, they add a valuable insight to the understanding of the relationship between records management and justice administration.

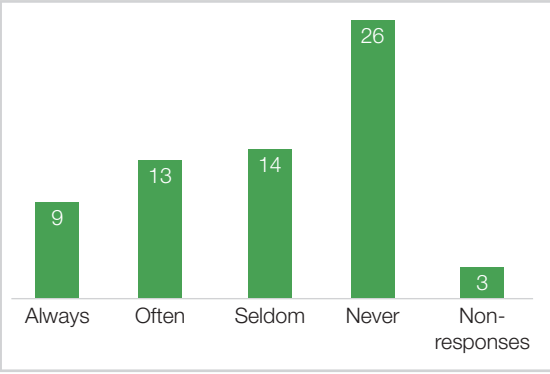
The objectives addressed by this paper are part of a wider study that surveyed the efficiency of electronic records management in Limpopo Province police stations for the effective administration of justice.

Results and discussion

E-docket system security

The respondents were asked to indicate how frequently the e-docket system was breached in the police stations in Limpopo Province with which they were familiar. An 'Always' response indicated a very high e-docket system vulnerability, whereas 'Never' indicated strong resistance to security breaches by the e-docket system. The results are depicted in Chart 1.

Chart 1: Perceived frequency of e-docket system breach (N=65)



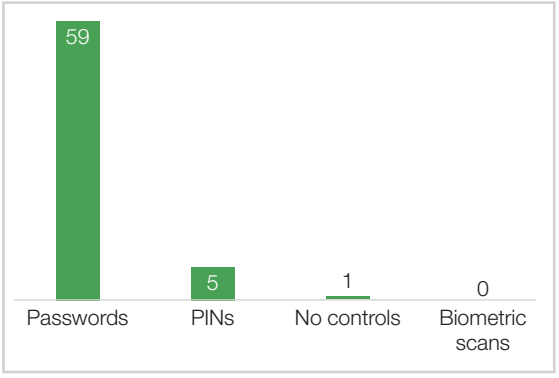
Electronic system security is intended to safeguard an organisation's records management infrastructure and records from modifications, misinterpretations, or loss.[56] Security is cited as one of the challenges of managing electronic records because such systems are at risk of experiencing disasters. In Botswana, for instance, inadequate security measures were among the challenges facing electronic record management.[57] The e-docket system in SAPS is not an exception.

As depicted in Chart 1, this study suggests that the e-docket system in the stations under review may be vulnerable to security breaches. This was evidenced by nine respondents (14%) who indicated that the e-docket system *always* suffers a security breach, thirteen (20%) who indicated that it occurs *often*, and fourteen (21%) out of 65 survey respondents who indicated that a security breach *seldom* occurred. Twenty-six respondents (40%) – a considerable number – said that the e-docket system was *never* breached. All responses considered, this implies a low technological readiness for secure electronic records management in the SAPS.

E-docket system access control

Access control is another important element of security in electronic records systems. Chart 2 displays the results when asking respondents about the access control measures employed for the e-docket system.

Chart 2: E-docket system access control measures



Some of the security-related threats facing records management include improper access to information, which can lead to unauthorised changes or modifications of records, a lack of control over the traceability of records, and unauthorised destruction of records.[58] In the case of the justice system, this may have far-reaching implications for the delivery of justice, as altered dockets can no longer be deemed authentic and admissible in court.

As depicted in Chart 2, the results show that the most predominant security measure used to regulate access to the e-docket system in these stations was *passwords*, which

received the support of 59 respondents (91%). Five respondents (7%) said Personal Identity Numbers (*PINs*) were used to regulate access to the e-docket system. The results clearly show that access to the e-docket system in these police stations was mainly regulated through passwords.

The downside of using passwords as the sole access control measure is that a password may be weak, or even copied by other colleagues with malicious intentions. Human-related threats are cited among the most common security risks with regard to access control of electronic information.[59] The most frequent types of information security breaches attributable to human actions in organisations include weak password choices, system configuration errors, access by individuals without authorisation, and insufficient knowledge.[60]

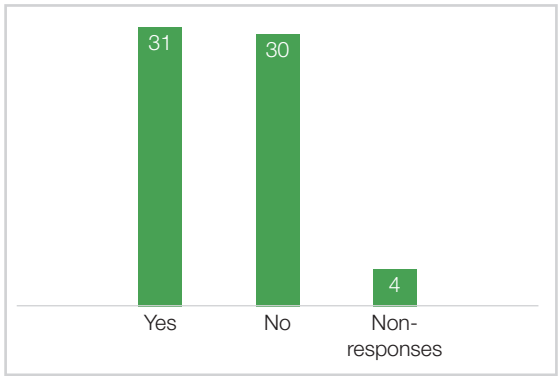
When access control is breached, the consequences can be serious. Compromises in the management of electronic records can result in suspects walking out of court free, or not being brought to court at all because dockets do not arrive on time or are not available. This makes it impossible for a judge or magistrate to pass judgment.[61] To further underline the severity of security breaches and technological disruptions on records management, another study found that cyber threats often led to incidents of system failure, which then resulted in wider disruption of service delivery.[62]

Information security ensures that an organisation's ICT systems, data, and infrastructure are protected from risks such as unauthorised access and manipulation, loss or destruction of data.[63] However, if organisations do not ensure that electronic records are managed properly through intelligent systems that provide constant intellectual and physical control, access control can never be achieved.[64]

Backup and recovery plan

Respondents were asked to use a Yes or No answer to indicate whether there was a backup and recovery plan for the e-docket system in their police station. Chart 3 depicts the responses.

Chart 3: Availability of records management backup plan



It is difficult to determine whether SAPS has a backup and recovery plan, as the respondents were almost equally divided on the question whether SAPS has a backup and recovery plan. As shown in Chart 3, 31 respondents (48%) supported the statement with a 'Yes', while 30 (46%) responded with a 'No'. This implies that the respondents may not know or understand what backup and recovery are about.

Respondents who answered 'Yes' were asked an open-ended follow-up question about what that consisted of. Six respondents indicated that there was a manual system as a backup plan in case the e-docket system failed. However, this is inadequate in the case of a disaster, unless copies of current records are kept off-site. Many organisations migrate to electronic records management due to the many limitations of manual systems. If these stations rely on on-site manual backup, they may well be susceptible to security risks of disaster and loss of electronic records.

A backup and recovery plan enables an organisation to develop strategies to minimise risks and restore its operations following a disaster.[65] A backup and recovery plan refers to a document that outlines what needs to be done by whom to protect electronic and paper-based records in any organisation. For electronic records, this includes an off-site backup of all stored information with a copy of the recovery plan.[66] A similar approach may be used for physical records. Backup data must be stored at a remote location that is different from the original creation and usage location.[67] The purpose of a backup and disaster recovery procedure is to reconstruct authentic and reliable records. It is thus essential that backup data includes associated metadata and audit trails of all records so that the authenticity of recovered records is not compromised.[68]

Proposed security framework

The study established that current security measures in these police stations may be open to being bypassed or breached, such that e-dockets are vulnerable to loss or change, whether accidental or malicious. It is imperative for electronic records to be protected against the numerous threats to their integrity and their very existence, prompting the need for improved system security and monitoring. Efficient management of e-records is critical to ensure the protection of vital records,[69] hence the proposed framework for improving security measures for electronic records on the e-docket system in these police stations, as depicted in Chart 4.

A comprehensive security approach for records would not only consider technical controls but also administrative and physical safeguards,[70] including training requirements. This framework is adopted from Ives (2014), who outlines these security pillars as ranging from techniques regarding the location of computers to the use of firewall software to protect digital records.[71]

Chart 4: Security control elements

Source: adopted from Kruse, Smith, Vanderlinden and Nealand, 2017

At an administrative level, security controls entail disaster management planning and putting backup systems in place.[72] Administrative controls would include policies, procedures and any other guidelines in written form. Clear security and disaster recovery policies and guidelines provide a basis for staff training on security control measures for records. Furthermore, owing to increased risks of disaster and electronic records loss, it is necessary to enforce a regular and clear backup and recovery plan in the police service.

Technical controls are also needed to guard the security of records. This aspect includes the use of role-based and personal-based authentication, such as passwords, firewalls, (RFI) tags, and usernames.[73] This can be a useful measure when coupled with other security control elements. Furthermore, technical security measures include hardware and software elements such as audit controls, provided for the security of information resources.[74] However, the SAPS needs to expand its security approach beyond technical safeguards in order to improve the efficiency of its electronic records management for effective justice delivery.

Physical controls would include all physical measures taken by an organisation to secure its records for the sake of administrative justice. Smoke and heat detectors and fire extinguishers are some of the physical measures records centres may take to detect and suppress potential records disasters.[75] To secure records against unauthorised access, manned security points, closed-circuit television cameras and burglar proofing every window can be instituted.[76] To increase the survivability of digital records in the event of natural or human-made disasters, power failures or other types of disruptions, organisations may adopt a distributed digital preservation strategy, where copies of digital files are distributed in server computers across geographically isolated areas.[77] Similarly, backup data must be stored at a remote location that is different from the original creation and usage location.

Finally, training is essential for the effective and efficient use of the e-docket system, as some security elements require specialised skill sets related to backup and recovery for the effective management of records.[78] This would clear the confusion on whether the current e-docket system has a backup and recovery plan. What needs to be considered is whether the backup of the e-docket system would allow it to be restored to full functionality in case of a disaster. Without training in and about the system, SAPS personnel may believe that the system cannot back up and recover data in the event of a disaster. Regular and compulsory training is essential to establish and maintain a level of awareness, commitment and enthusiasm among records handling staff.[79] Not all police officers need to know how to restore a crashed system. However, having specific records management personnel trained to assist with backup recovery is essential. Training may be in the form of in-house workshops, mock-up drills and seminars. Therefore, staff training needs to be included in preparation for disasters and management of access control to records. For any disaster management plan to succeed, staff need to be made aware of their mandate, should disaster strike.[80]

Conclusion

The implementation of electronic records management programmes, such as the e-docket system in the SAPS, is undoubtedly a major step forward in rendering proper administration of justice to citizens. However, without adequate security, access controls and backup of records on the e-docket system, unauthorised access to records or loss may result. The potential risks and consequences of data loss or unauthorised access include delays in court proceedings, criminals walking free due to a lack of evidence, and victims of crime not receiving justice. The legal implications are that the SAPS may have civil claims lodged against it for such data breaches and privacy violations. Therefore, the quality of the management system adopted for recordkeeping has a direct effect on the ability or inability of the SAPS to administer justice to citizens.

The study revealed that access to the e-docket system in these stations in Limpopo Province was predominantly secured through passwords, which have been proven to be an inadequate security mechanism if a weaker password is used. Similarly, the use of a manual system as a backup and recovery measure for electronic records is not a good security measure in the event of a disaster, unless stations use off-site storage to keep their records. The flow of the docket from the police stations to the courtroom is vulnerable to risks that may violate the rights of persons and compromise the provision of justice.

The researchers conclude by recommending further study on how the current system has evolved from paper-based records, paying particular attention to the potential benefits of transitioning to the direct capture of dockets

on computers. Such a shift could save time and resources by reducing the need for manual processes and scanning. They also recommend further research on the use of Artificial Intelligence (AI) for effective docket management in the SAPS. The inroads made since the advent of AI suggest that it can enhance data security by detecting unusual patterns and potential threats in real time, enabling proactive responses. AI may also employ encryption techniques to protect confidential records from unauthorised access. Still, without proper security protections, the information may be accessed by others, threatening the privacy of the owners of that information.

Notes

1 Alex Lesiba Legodi is a lecturer at the Department of Information Science at the University of South Africa. Maoka Andries Dikotla is an Associate Professor in the Department of Information Science at the University of South Africa.

2 Amos Shibambu and Mpho Ngoepe, When rain clouds gather: Digital curation of South African public records in the cloud, *South African Journal of Information Management* 22(1) (2020), 1–9.

3 Kameshwhri Moonsamy, Analysis of the administration and governance of the South African case docket, Master's thesis, University of Cape Town, 2018; K Ntengenyane and F Khayundi, Harnessing a records management programme for justice delivery at the Alice magistrate court in the Eastern Cape Province, South Africa, *Journal of the South African Society of Archivists* 54 (2021), 12–23.

4 South African Police Service, Case Docket Analysis Learner Manual, Pretoria: Government Printer, 2002, 2.

5 South African Law Commission, Discussion paper on sentencing: A compensation scheme for victims of crime in South Africa, Pretoria: Government Printer, 2001, 92.

6 *Wolf v S* – Ruling (16/2022)[2023] ZAECQBHC 62 (20 October 2023).

7 Ntengenyane and Khayundi, Harnessing a records management programme for justice delivery, 13–23.

8 D Teffo and KG Chuma, Management of electronic records to support judicial systems at Temba Magistrates' Court in the North West Province of South Africa, *Journal of the South African Society of Archivists* 56 (2023), 23–35, https://orcid.org/0000-0002-5817-6063.

9 Kabelo Given Chuma and Mpho Ngoepe, Security of electronic personal health information in a public hospital in South Africa, *Information Security Journal: A Global Perspective* 31(2) (2022),179–195.

10 AL Legodi and DMA Dikotla, E-docket system for improved administration and justice delivery in selected Limpopo province police stations, *Journal of the South African Society of Archivists* 55 (2022), 27–40.

11 Bilkis Omar, The SAPS e-docket system, *ISS Today*, 2009.

12 See saps.gov.za. South African Police Service, 2018, https://www.saps.gov.za/about/about.php (Accessed 7 January 2022).

13 Nikhat Akhtar, Bedine Kerim, Yusuf Perwej, Anurag Tiwari and Sheeba Praveen, A comprehensive overview of privacy and data security for cloud storage, *International Journal of Scientific Research in Science Engineering and Technology* (2021), 113–152; Ken Guo, Junlian Xiang, Norm Archer, Susan Sproule and Yufei Yuan, Chapter 1 Introduction in Identity Theft and Fraud: Evaluating and Managing Risk, Ottawa: University of Ottawa Press, 2012, 1–13, https://doi.org/10.1515/9780776619927-001.

14 Chuma and Ngoepe, Security of electronic personal health information.

15 DPP Law, Legal liabilities under the Data Protection Act 2018 for breaches, including theft, loss, or unlawful disclosure, 2025, available at: https://www.dpplaw.co.uk/news/legal-liabilities-under-the-data-protection-act-2018 (accessed 25 April 2025).

16 Abualkishik, Abedallah Zaid, Ali A Alwan and Yonis Gulzar, Disaster recovery in cloud computing systems: an overview, *International Journal of Advanced Computer Science and Applications*, 11(9) (2020), http://dx.doi.org/10.14569/IJACSA.2020.0110984.

17 Ibid.

18 A Usman, AU Hafiz, S Ammar and UIA Zain, Government cloud adoption and architecture, Proceedings of the ICCMET, China, 2019.

19 L Kibe, Impact of cloud-based services on records management in public organisations in Kenya, paper presented at the First International Conference on Information and Knowledge Management, Nairobi, August 2016, 125, available at: https://www.researchgate.net/publication/307569275_Impact_of_cloud_base (accessed 25 April 2025).

20 R Mugyenyi, Adoption of cloud computing services for sustainable development of commercial banks in Uganda, *Global Journal of Computer Science and Technology: Cloud and Distributed* 18(1) (2018), 1–10.

21 Lungelo Sanele Mbatha, Lungile P Luthuli and Maggie Masenya Tlou, Prison breakthrough: Use of information systems in correctional facilities, 2020.

22 International Records Management Trust, 2004, *e-records readiness tool*, United Kingdom: s.n.

23 Moonsamy, Analysis of the administration and governance of the South African case docket.

24 Mpho Ngoepe, Records management models in the public sector in South Africa: Is there a flicker of light at the end of the dark tunnel?, *Information Development* 32(3) (2016), 338–353.

25 Aliza Ismail and Jamaludin Adnan, Towards establishing a framework for managing trusted records in the electronic environment, Records Management Journal 19(2) (2009), 135–146.

26 Legodi and Dikotla, E-docket system for improved administration and justice delivery, 27–40.

27 S Smillie, Rolling out of SAPS's e-docket system to replace archaic 'brown donkeys' drags on, 2020, available at: https://www.dailymaverick.co.za/article/2020-02-12-rolling-

out-of-saps-e-docket-system (accessed 17 December 2020).

28 National Archives and Records Service of South Africa, Managing Electronic Records in Governmental Bodies: Policy, Principles and Requirements, Pretoria: National Archives and Records Service of South Africa, 2006.

29 Anahí Casadesús de Mingo and Agustí Cerrillo-i-Martínez, Improving records management to promote transparency and prevent corruption, *International Journal of Information Management* 38(1) (2018), 256–261.

30 Mbatha, Luthuli and Tlou, Prison breakthrough.

31 M Konstantinos, Records management and electronic records management opportunities and limitations: A case study in Greek companies, Dissertation (Masters), Department of Informatics, Linnaeus University, 2015, (accessed April 2021).

32 Legodi and Dikotla, E-docket system for improved administration and justice delivery.

33 Ibid.

34 CAT Murray, MEC Albert Fritz on e-docket software not being effectively used by SAPS and courts, Western Cape Community Safety, 5 March 2020, available at: http://www.gov.za/speeches/r6135-million-e-docket-software-not-being-effectively-used (accessed 30 July 2020).

35 eDocket to improve police admin, SAnews.gov.za, 11 August 2017, available at: https://www.sanews.gov.za/south-africa/edocket-improve-police-admin (accessed 13 August 2020).

36 Moonsamy, Analysis of the administration and governance of the South African case docket.

37 S Smillie, Rolling out of SAPS's e-docket system.

38 TE Ives, The new 'E-Clinician' guide to compliance, *Audiology Today* 26(1) (2014), 52–53.

39 National Archives and Records Service of South Africa.

40 Trevor Moatlhodi and Trywell Kalusopa, An assessment of e-records readiness at the Ministry of Labour and Home Affairs, Gaborone, Botswana, *Mousaion* 34(3) (2016), 1–22.

41 Constant Okello-Obura, Effective records and information management as a catalyst for fighting corruption, *Information Development* 29(2) (2013), 114–122.

42 Qiuhui Xiao, Xu Xiaotong and Liu Panpan, Security status of electronic records preservation in central China: The survey results of 34 archives in Wuhan City, *Library Hi Tech* 39(1) (2021), 22–36.

43 Legodi and Dikotla, E-docket system for improved administration and justice delivery.

44 Ngoako Solomon Marutha, Framework for Medical and Health Records Management Skills and Competency Development in Limpopo Public Hospitals to Support Healthcare Service Delivery in the Digital Era, *African Journal of Library, Archives & Information Science* 29(2) (2019).

45 Erasmus Nyanga, CT Nengomasha and CM Beukes-Amiss, Disaster Preparedness and Management at the National Archives and the National Library of Namibia, *African Journal of Library, Archives & Information Science* 28(1) (2018); South African National Standard 15801: 2005, Electronic imaging – Information stored electronically – Recommendations for trustworthiness and reliability, Pretoria: South African Bureau of Standards, 2005.

46 S Suguna and A Suhasini, Overview of data backup and disaster recovery in cloud, in *Proceedings of the International Conference on Information Communication and Embedded Systems* (ICICES2014), IEEE, 2014, 1–7.

47 Heather Brown, Managing disaster preparedness and response for hybrid collections in Australian national and state libraries, *Journal of the Australian Library and Information Association* 67(4) (2018), 411–433.

48 National Archives and Records Service of South Africa.

49 Elsebah Maseh and Stephen Mutula, Records management readiness for open government in the Kenyan judiciary, *Mousaion* 34(3) (2016), 146–166.

50 Ngoepe, Records management models in the public sector in South Africa, 338–353.

51 Elizabeth Shepherd, Managing electronic records, *Records Management Journal* 4(1) (1994), 39–49.

52 National Archives and Records Service of South Africa.

53 Cederberg Local Municipality, ICT data backup and recovery policy: Backup and recovery, Cederberg, 2018.

54 Ntengenyane and Khayundi, Harnessing a records management programme for justice delivery.

55 A Bryman, Social research methods, 4th ed, New York: Oxford University Press Inc., 2012.

56 A Ismail and A Jamaludin, Towards establishing a framework for managing trusted records in the electronic environment, *Records Management Journal* 19(2) (2009), 135–146, https://www.doi.org/10.1108/09565690910972084

57 Donald Rakemane and Batlang C Serema, Electronic records management practices at the Companies and Intellectual Property Authority in Gaborone, Botswana, *Journal of the South African Society of Archivists*, 51 (2018) 148–169; Trywell Kalusopa, Extent of the integration of information communication and technology (ICT) systems in the management of records in labour organisations in Botswana, *Journal of the South African Society of Archivists* 49 (2016), 102–115.

58 AC De Mingo and AC Martinez, Improving records management to promote transparency and prevent corruption, *International Journal of Information Management* 38(1) (2018), 256–261, https://doi.org/10.1016/j.ijinfomgt.2017.09.005.

59 Chuma and Ngoepe, Security of electronic personal health information.

60 Ibid.

61 M Ngoepe and S Makhubela, Justice delayed is justice denied: records management and the travesty of justice in South Africa, *Records Management Journal* 25(3) (2015), 288–305; C Presence, Dockets missing so suspects walk free, 2014. [Online] Available at: https://www.iol.co.za/news/dockets-missing-so-suspects-walk-1643148 (Accessed 10 June 2024).

62 Chuma and Ngoepe, Security of electronic personal health information.

63 Cederberg Local Municipality.

64 Justus Wamukoya and Stephen Mutula, E-records management and governance in East and Southern Africa, *Malaysian Journal of Library & Information Science* 10(2) (2005), 67–83.

65 Brown, Managing disaster preparedness and response.

66 Ibid.

67 Zulkipli, Fatin Nur, Disaster preparedness for records management: a conceptual review, *Journal of Information and Knowledge Management* (JIKM) 11(1) (2021), 1–14.

68 Ibid.

69 Moatlhodi and Kalusopa, An assessment of e-records readiness.

70 CS Kruse, B Smith, H Vanderlinden and A Nealand, Security techniques for the electronic health records, *Journal of Medical Systems* 41(8) (2017), 127, https://doi.org/10.1007/s10916-017-0778-4.

71 Ives, The new 'E-Clinician' guide, 52–53.

72 C Asamoah, H Akussah, and A Musah, Recordkeeping and disaster management in public sector institutions in Ghana, *Records Management Journal*, 28(3) (2018), 218–233, https://doi.org/10.1108/RMJ-01-2018-0001.

73 Kruse et al, Security techniques.

74 Chuma and Ngoepe, Security of electronic personal health information.

75 Asamoah, Akussah and Adams, Recordkeeping and disaster management.

76 Ibid.

77 Aaron Trehub, Corey Davis, Mark Jordan, Cinda May and Sam Meister, LOCKSS Networks: Community-based digital preservation, *Digital Preservation in Libraries: Preparing for a Sustainable Future (An ALCTS Monograph)*, 2019.

78 Brown, Managing disaster preparedness and response.

79 John McIlwaine and Marie-Thérèse Varlamoff, *IFLA disaster preparedness and planning: A brief manual*. IFLA PAC, Paris, 2006.

80 Asamoah, Akussah and Adams, Recordkeeping and disaster management.