Kabarak Journal of Research & Innovation Volume 16 Number 3 (2026)
ISSN 2305-784X (print) ISSN 2410-8383 (online)
https://journals.kabarak.ac.ke/index.php/kjri/

Access Control Strategy On Administrative Process Performance In Government Entities In Nakuru County

Authors
Juliet A. W. Mwangi and Daisy J. C. Bowen

Affiliation
School of Business and Economics, Kabarak University, Private Bag, Nakuru, Kenya.

Corresponding Author
Juliet A. W. Mwangi – E-mail: anastasiajwanjiku@gmail.com

Article History: Submitted: 11th August 2026; Accepted: 3rd November 2026; Published (online): 9th November 2026

Abstract

The increasing adoption of government digital systems such as IFMIS, UHRIS, and eCitizen has expanded the use of digital technologies in administrative processes while increasing the need to safeguard sensitive data against unauthorized access and misuse. Although access control is an important component of organizational data security, its contribution to administrative process performance within Kenyan government entities remains insufficiently examined. This paper presents a focused analysis of access control strategy from a broader study of data security strategies and administrative process performance in government entities in Nakuru County, Kenya. A descriptive cross-sectional design employing a census approach targeted 60 respondents comprising 27 ICT officers and 33 heads of sections across nine government entities. Data were collected using a structured questionnaire, yielding 48 valid responses and an 80% usable response rate. Descriptive statistics and multiple linear regression were used for analysis. Access control implementation was generally rated favorably ($M = 3.82$, $SD = 0.81$). The overall regression model incorporating data encryption, access control, network defense, and security training and awareness strategies was statistically significant, $F(4, 43) = 36.809$, $p < .001$, explaining 77.4% of the variance in administrative process performance ($R^2 = .774$). However, after controlling for the other data security strategies, access control strategy made a positive but statistically nonsignificant unique contribution to administrative process performance ($B = .174$, $\beta = .159$, $p = .258$). The findings suggest that access control should be considered within the broader organizational data security environment rather than as an independent determinant of administrative process performance. The study recommends that Government entities should sustain established access control practices while strengthening comparatively lower-rated areas, particularly employee training, independent compliance reviews, and incident response procedures.

Keywords
Access Control Strategy; Administrative Process Performance;Government Entities

Introduction

Governments worldwide are increasingly relying on digital systems to manage administrative processes and deliver public services. Systems supporting financial management, human resource administration, records management, regulatory compliance, and citizen services

have become central to contemporary public sector operations. Digital transformation has reshaped administrative processes through more timely data processing and greater integration of digital technologies into government operations(Organisation for Economic Co-operation and Development [OECD], 2020; Dener et al., 2021). However, growing dependence on digital systems has also created a greater need to protect sensitive government data and systems against cybersecurity threats, including unauthorized access.

Such incidents may compromise data confidentiality and integrity and disrupt administrative processes. Consequently, access control has become an important component of data security for regulating access to digital systems according to predefined roles, responsibilities, and authorization levels. Access control mechanisms such as user authentication, authorization, least-privilege principles, and audit logging help restrict inappropriate access and safeguard organizational data (National Institute of Standards and Technology [NIST], 2020; ISO/IEC, 2022).

Globally, government institutions continue to face cybersecurity threats involving unauthorized access, credential compromise, and misuse of credentials or privileges. Such threats may compromise government digital systems, disrupt operations, and affect data integrity (European Union Agency for Cybersecurity [ENISA], 2024; Verizon, 2024). Access controls based on identity verification, authorization, least privilege, and monitoring are therefore important for restricting inappropriate access and supporting secure organizational operations (NIST, 2020; ISO/IEC, 2022). From the employee perspective, Alraja et al. (2023) identified behavioral factors, including role values, as relevant to employees' intentions to comply with information security policies, highlighting the human dimension of organizational security alongside technical controls.

In Sub-Saharan Africa, institutional and technical constraints, including limited cybersecurity capacity, uneven implementation of security measures, inadequate digital infrastructure, and governance challenges, continue to affect the implementation of data security measures, including access control(World Bank, 2023; International Telecommunication Union [ITU], 2024). These constraints may increase exposure to unauthorized access and data misuse, potentially affecting the management of administrative processes in government entities.

In Kenya, digital transformation initiatives such as the Integrated Financial Management Information System (IFMIS), Unified Human Resource Information System (UHRIS), and eCitizen platform have transformed the management of administrative processes in government entities. The Data Protection Act, 2019 provides a legal framework for the protection of personal data (Republic of Kenya, 2019), while the Government ICT Standards and Guidelines establish security requirements for government digital systems, including access management and data protection (Information and Communication Technology Authority [ICTA], 2023).Despite these developments, the national cybersecurity monitoring continues to document cybersecurity threats affecting Kenya's digital environment (National KE-CIRT/CC, 2024). Weak implementation of access control practices may increase exposure to unauthorized access and undermine the effectiveness of organizational security controls (Alraja et al., 2023).

At the county level, the growing use of digital systems underscores the need for effective implementation and monitoring of access control practices. However, differences in technical capacity, available resources, and implementation of security measures may affect how

consistently access controls are applied across government entities. Previous studies have examined access control implementation and management across organizations (Yaokumah&Okai, 2018), as well as identity management and authorization practices (Mollakuqe& Dimitrova, 2024). However, these studies did not specifically examine the unique contribution of access control strategy to administrative process performance when considered alongside other organizational data security strategies. This leaves an empirical gap concerning the relationship between access control strategy and administrative process performance in Kenyan government entities. Addressing this gap is particularly relevant to government entities in Nakuru County, where the study examines access control strategy within the broader context of organizational data security.

This study is anchored in Contingency Theory (Lawrence & Lorsch, 1967), which proposes that organizational effectiveness depends on the alignment between organizational arrangements and the conditions within which organizations operate. The theory rejects the assumption that a single organizational practice is universally effective and instead emphasizes the importance of contextual fit. Applied to data security, the contribution of access control strategy to administrative process performance may depend on institutional capacity, technological infrastructure, organizational requirements, employee capabilities, and the implementation of complementary security strategies.Contingency Theory therefore provides an appropriate framework for examining the unique contribution of access control strategy while accounting for other data security strategies within government entities in Nakuru County.

The study's objective was to examine the contribution of access control strategy to administrative process performance in government entities in Nakuru County, Kenya. It hypothesized that access control strategy does not make a statistically significant unique contribution to administrative process performance after accounting for other data security strategies. By examining this contribution within a multivariable framework, the study provides empirical evidence on the role of access control strategy in administrative process performance within Kenyan government entities.

Methodology

The study adopted a descriptive cross-sectional research design to examine the contribution of access control strategy to administrative process performance in government entities in Nakuru County, Kenya. The design was appropriate for assessing respondents' perceptions of the study variables at a single point in time and examining their statistical relationships.

The target population comprised 60 respondents drawn from nine government entities, including 27 ICT officers and 33 heads of sections. A census approach was adopted because the target population was small and manageable; therefore, all eligible respondents were invited to participate. A total of 51 questionnaires were received. Following screening for completeness, adherence to the anonymous respondent-code format, and response quality, three questionnaires were excluded, leaving 48 valid questionnaires for analysis. This represented an 80% usable response rate.

Primary data were collected using a structured self-administered questionnaire comprising five-point Likert-scale items measuring the four data security strategies and administrative

process performance. Access control strategy was measured using items relating to periodic user access reviews, audit logging, access control policies, multi-factor authentication, compliance evaluation, incident response, employee training, and prevention of unauthorized access.

Because the present paper was derived from a broader study, the regression model also included data encryption strategy, network defense strategy, and security training and awareness strategy as additional predictors. Administrative process performance constituted the dependent variable. Composite scores for the respective constructs were derived from their corresponding questionnaire items, with higher scores representing stronger implementation of the respective data security strategy or higher perceived administrative process performance.The instrument was pilot-tested in Nyandarua County using six respondents drawn from institutions comparable to those included in the main study. The access control strategy construct achieved a Cronbach's alpha coefficient of .753, indicating acceptable internal consistency.
Theregression model was specified as follows:

$$Y=\beta_0+ \beta_1X_1 + \boldsymbol{\beta_2}\mathbf{X_2}+ \beta_3X_3 + \beta_4X_4 +\varepsilon$$

Where:

Y= Administrative Process Performance
β_0 = Regression constant (intercept)
β_1 –β_4= Regression coefficients for the independent variables
X_1 =Data Encryption Strategy
X_2= Access Control Strategy
X_3 = Network Defense Strategy
X_4 = Security Training and Awareness Strategy
ε = Error term

Prior to regression analysis, relevant diagnostic tests were conducted. Multicollinearity was assessed using variance inflation factor (VIF) and tolerance statistics. VIF values ranged from 2.112 to 3.650, while tolerance values ranged from .274 to .473, indicating that severe multicollinearity was not evident among the predictor variables. Normality of the regression residuals was assessed using the Shapiro–Wilk test. The residuals did not significantly depart from normality (W = .980, p = .576), indicating that the normality assumption for the regression model was satisfied.

Ethical Considerations

The study adhered toestablished ethical principles to protectparticipants' rights, dignity, privacy, and well-being. Ethical approval was obtained from the Kabarak University Research Ethics Committee (KUREC)**,** and a research permit was obtained from the National Commission for Science, Technology and Innovation (NACOSTI) before data collection commenced. Institutional authorization was subsequently obtained from the participating government entities.

Before participating in the study, participants were provided with information explaining the purpose of the study, the voluntary nature of their participation, and their right to withdraw at any stage without penalty. Informed consent was obtained electronically through a consent

statement presented at the beginning of the questionnaire, which participants were required to acknowledge before proceeding.

The study involved minimal risk to participants. The questionnaire was designed to collect responses using anonymous respondent codes rather than personal identifiers, and all valid responses were treated anonymously and kept strictly confidential. Data were stored on password-protected and encrypted electronic devices accessible only to the researcher. The data will be retained securely for two years following completion of the study and permanently deleted thereafter in accordance with institutional data retention policies.

Results

Descriptive Results

Descriptive statistics were computed to assess the implementation of access control strategyin the government entities. Table 1 presents respondents' perceptions of the implementation ofaccess controlstrategy.

Table 1

Descriptive Statistics for Access Control Strategy

Statement	1	2	3	4	5	*M*	*SD*
User access levels are reviewed periodically to prevent unauthorized access.	4 (8.3%)	2 (4.2%)	7(14.6%)	16(33.3%)	19(39.6%)	**3.92**	**1.22**
System audit logs accurately record all user access and modifications.	3(6.2%)	4 (8.3%)	4 (8.3%)	15 (31.2%)	22 (45.8%)	**4.02**	**1.21**
Access control policies ensure the confidentiality and integrity of data.	0 (0.0%)	3 (6.2%)	3 (6.2%)	16 (33.3%)	26(54.2%)	**4.35**	**0.86**
Multi-factor authentication is implemented to enhance security.	3 (6.2%)	4 (8.3%)	8(16.7%)	16 (33.3%)	17(35.4%)	**3.83**	**1.19**
Access control compliance is routinely evaluated through independent reviews.	4 (8.3%)	8(16.7%)	13(27.1%)	14 (29.2%)	9 (18.8%)	**3.33**	**1.21**
Incident response procedures for access control violations are effective.	2 (4.2%)	6(12.5%)	13(27.1%)	17 (35.4%)	10(20.8%)	**3.56**	**1.09**
Adequate training is provided on access control policies.	4 (8.3%)	9 (18.8%)	12 (25.0%)	16 (33.3%)	7 (14.6%)	**3.27**	**1.18**
Access control measures reduce unauthorized access to sensitive data.	2 (4.2%)	1 (2.1%)	4 (8.3%)	16 (33.3%)	25(52.1%)	**4.27**	**1.01**
Overall Mean						**3.820.81**	

Note.1=Strongly Disagree;2=Disagree; 3=Undecided; 4=Agree;5=Strongly Agree;M=mean; SD= standarddeviation

The overall mean score for access control strategy was 3.82 (SD = 0.81)**,** indicating generally favorable perceptions of the implementation of access control measures across the government entities. The highest-rated component was access control policies aimed at ensuring the confidentiality and integrity of data **(**M = 4.35, SD = 0.86**),** followed by access control measures for reducing unauthorized access to sensitive data **(**M = 4.27, SD = 1.01**)**

and the accuracy of system audit logs in recording user access and modifications (M = 4.02, SD = 1.21).

The lowest mean score was recorded for adequate training on access control policies (M = 3.27, SD = 1.18), followed by routine evaluation of access control compliance through independent reviews (M = 3.33, SD = 1.21**)** and the effectiveness of incident response procedures for access control violations (M = 3.56, SD = 1.09**).** Overall, the findings indicate that access control measures were generally perceived as being implemented across the government entities, particularly those relating to data confidentiality and integrity, prevention of unauthorized access, and system audit logging. However, the comparatively lower ratings for employee training, independent compliance reviews, and incident response procedures indicate areas where implementation could be strengthened.

RegressionResults

Table 2 presents the overall model summary for the regression analysis.The regression model produced a multiple correlation coefficient of R = .880, indicating a strong overall relationship between the combined data security strategies and administrative process performance. The coefficient of determination, R^2 = .774, indicates that data encryption, access control, network defense, and security training and awareness strategies jointly explained 77.4% of the variance in administrative process performance.

Table 2

Model Summary for the Regression Analysis

Model	*R*	R^2	Adjusted R^2	Std. Error of the Estimate
1	.880	.774	.753	.440

The ANOVA results in Table 3 which were used to determine the overall statistical significance of the regression model, indicate that the overall regression model was statistically significant, F(4, 43) = 36.809, p < .001. This indicates that the four data security strategies, when considered jointly, significantly predicted administrative process performance.

Table 3

Analysis of Variance (ANOVA) for the Regression Model

Model	Sum of Squares	*df*	Mean Square	*F*	*P*
Regression	28.480	4	7.120	36.809	<.001
Residual	8.317	43	0.193		
Total	36.797	47			

Table 4 presents the regression coefficients for the individual predictors included in the model.

Access control strategy had a positive but statistically nonsignificant unique contribution to administrative process performance (B = .174, β = .159, t = 1.147, p = .258). Holding data

encryption, network defense, and security training and awareness strategies constant, a one-unit increase in the access control strategy score was associated with a .174-unit increase in the administrative process performance score.However, this unique contribution was notstatistically significant (p = .258); therefore, the nullhypothesis was notrejected**.**

Table4
Regression Coefficients Predicting Administrative Process Performance

Predictor	*B*	Std. Error	*β*	*t*	*p*
Constant	.365	.349	—	1.046	.302
Data Encryption Strategy (X_1)	.092	.114	.085	.810	.422
Access Control Strategy (X_2)	**.174**	**.152**	**.159**	**1.147**	**.258**
Network Defense Strategy (X_3)	-.070	.160	-.058	-.435	.665
Security Training & Awareness Strategy (X_4)	.744	.120	.740	6.195	<.001

Discussion

The study examined whether the implementation of access control practices was associated with administrative process performance in government entities in Nakuru County. Access control was assessed through practices such as periodic user access reviews, system audit logging, access control policies, multi-factor authentication, compliance evaluation, incident response, employee training, and measures for preventing unauthorized access. The findings showed generally favorable perceptions of access control implementation across the government entities. However, access control strategy had a positive but statistically nonsignificant unique contribution to administrative process performance after accounting for data encryption, network defense, and security training and awareness strategies.This means that, although better implementation of access control was associated with higher administrative process performance in the estimated model, the evidence was insufficient to conclude that access control independently explained differences in administrative process performance once the other data security strategies were considered.

The findings can be considered in relation to Yaokumah and Okai (2018), who examined the implementation and management of access control security measures across organizations in Ghana, focusing on access control policy, user access management, user responsibility and accountability, and system and application access control. Their study highlighted the importance of considering access control not only as a technical mechanism but also in terms of its organizational implementation and management. The generally favorable perceptions of access control implementation in the present study similarly demonstrate the importance of considering how access control policies and practices are implemented within organizational settings. However, the nonsignificant unique contribution of access control after accounting for the other data security strategies suggests that its relationship with administrative process performance should be considered within the broader organizational data security environment rather than as an isolated determinant.

The findings also relate to Alraja et al. (2023), who examined factors influencing employees' intentions to comply with information security policies and identified employee-related factors, including role values, as relevant to security policy compliance. Although their study

focused on information security policy compliance rather than access control or administrative process performance specifically, it highlights the human dimension in implementing organizational security requirements. In the present study, adequate training on access control policies was the lowest-rated access control measure.Although respondents generally viewed access control implementation favorably, the comparatively lower rating for employee training indicates that employee-related access control practices warrant further institutional attention alongside technical and administrative controls.

Similarly, Parkinson and Khan (2023) emphasized the importance of routinely analyzing access control policies and permissions to identify potentially problematic access rights that could expose organizational resources to unauthorized access, data theft, or unintended modification. This is relevant to the present study, in which periodic user access reviews were rated favorably. Respondents also reported favorable perceptions of access control policies for safeguarding data confidentiality and integrity and of system audit logging. These findings highlight the importance of sustaining effective implementation and monitoring of access control practices within government entities.
The findings further align with Mollakuqe and Dimitrova (2024), who demonstrated that effective identity management, authentication, authorization, and access governance reduce unauthorized access and strengthen organizational security. While their study focused on higher education institutions, the present studyprovidesrelated evidence withinthe Kenyan government context.

Overall, the findings underscore the importance of access control as both a technical security measure and an organizational practice within government entities. While measures relating to data confidentiality and integrity, prevention of unauthorized access, system audit logging, and periodic user access reviews were rated favorably, comparatively lower ratings were recorded for employee training, independent compliance reviews, and incident response procedures. Strengthening these comparatively lower-rated areas while sustaining the more favorably rated access control practices may enhance the implementation of access control and support administrative process performance within the broader organizational data security environment.

The findings can also be considered within the propositions of Contingency Theory (Lawrence & Lorsch, 1967), which posits that organizational effectiveness depends on the alignment of organizational practices with contextual conditions. From this perspective, the nonsignificant unique contribution of access control strategy does not necessarily imply that access control is unimportant to administrative process performance. Rather, its relevance may depend on how access control practices operate alongside other data security strategies and how well they are aligned with institutional requirements, technological infrastructure, user responsibilities, and organizational security policies.

Unlike studies that have concentrated primarily on technical access control models, security policy compliance, or other institutional settings, the present study provides evidence from government entities in Nakuru County, Kenya. The findings therefore contribute context-specific evidence showing that access control was generally perceived as being implemented across the government entities, although it did not make a statistically significant unique contribution to administrative process performance after accounting for the other data security strategies included in the model.

The findings should, however, be interpreted in light of the study's limitations. The study was conducted among selected government entities in Nakuru County, which limits the extent to which the findings can be generalized to other public-sector contexts. The use of self-reported questionnaire data may also have introduced response bias. In addition, the instrument was pilot-tested using a relatively small sample of six respondents in Nyandarua County. Although the access control strategy scale recorded an acceptable Cronbach's alpha coefficient ($\alpha = .753$), the small pilot sample limits the stability and precision of this reliability estimate and should therefore be considered when interpreting the instrument's reliability. Furthermore, because the study employed a cross-sectional design, the observed relationships should not be interpreted as definitive evidence of causality.

Conclusion

This study examined the contribution of access control strategy to administrative process performance in government entities in Nakuru County, Kenya. The findings showed that access control strategy made a positive but statistically nonsignificant unique contributionto administrative process performance after controlling for the other data security strategies included in the study. Therefore, the evidence was insufficient to conclude that access control independently predicted administrative process performance within the multivariable model.The study further established that access control measures were generally perceived as being implemented across the government entities, particularly those relating to safeguarding data confidentiality and integrity, preventing unauthorized access to sensitive data, system audit logging, and periodic review of user access levels**.** Comparatively lower ratings for employee training, independent compliance reviews, and incident response procedures indicate areas where access control implementation could be strengthened.

Overall, the study contributes context-specific evidence on the implementation of access control and its relationship with administrative process performance in government entities in Nakuru County. Although access control did not make a statistically significant unique contribution to administrative process performance after accounting for the other data security strategies, its implementation remains an important component of the broader organizational data security environment. Sustaining well-established access control practices while strengthening comparatively lower-rated areas may support secure and effective administrative processes within government entities.

Recommendations

At the policy level, government entities should regularly review and strengthen institutional access control policies to provide clear requirements for user authentication, authorization, periodic access reviews, multi-factor authentication, monitoring of user access, and response to access violations. The policies should clearly define responsibilities for implementation, compliance monitoring, and enforcement. Particular attention should be given to areas where implementation was comparatively lower, including employee training, independent compliance reviews, and incident response procedures**.** Strengthening these areas would provide a more consistent governance framework for managing access to sensitive data and supporting secure and effective administrative processes.

At the management level, government entities should ensure that access control policies are consistently implemented, monitored, and communicated to staff. Existing strengths in safeguarding data confidentiality and integrity, preventing unauthorized access, system audit logging, and periodic user access reviews should be sustained. Greater attention should be

given to employee training, independent compliance reviews, and procedures for responding to access control violations. Regular reviews should be conducted to ensure that employees retain only the access required for their roles and that inappropriate or outdated access privileges are identified and addressed. Management should also ensure that technical access controls are supported by appropriate staff training, monitoring, compliance oversight, and clearly defined accountability mechanisms.

Future research should examine access control strategy and administrative process performance in government entities in other counties and at the national government level to determine whether similar findings are observed across different public-sector contexts. Longitudinal studies could also examine how changes in access control implementation relate to administrative process performance over time, thereby providing stronger evidence regarding the direction of the relationship.Further research could examine organizational factors, such as management support, institutional capacity, and security culture, as well as the interaction of access control with other data security strategies, to better understand the conditions under which access control may contribute to administrative process performance.

Declarations

Acknowledgements
The first author gratefully acknowledges the encouragement and support received from colleagues and family members during the course of this study.

Author Contribution
Juliet A. W. Mwangi: Conceptualization, Methodology, Investigation, Writing – Original Draft
Jeptepkeny Bowen: Supervision, Formal Analysis, Writing – Review & Editing, Validation.
Both authors reviewed and approved the final version of the manuscript.

Funding Statement
The authors declare that this research received no external funding.

Declaration of Competing Interests
The authors declare no conflict of interest.

Research Approval
Ethical approval for this study was obtained from the Kabarak University Research Ethics Committee (KUREC) Ref. No. KABU01/KUREC/001/08/09/25 and research permit obtained from the National Commission for Science, Technology and Innovation (NACOSTI) Ref. No. 469042.

Licensing Statement
© 2026 The Author(s). This article is published by *Kabarak Journal of Research & Innovation (KJRI)* under the **Creative Commons Attribution 4.0 International (CC BY 4.0) License**, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and source are credited.

References

Alraja, M. N., Butt, U. J., &Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security, 129*, 103208. https://doi.org/10.1016/j.cose.2023.103208

Dener, C., Nii-Aponsah, H., Ghunney, L. E., & Johns, K. D. (2021). *GovTech maturity index: The state of public sector digital transformation* (International Development in Focus). World Bank. https://doi.org/10.1596/978-1-4648-1765-6

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

International Telecommunication Union. (2024). *Global cybersecurity index 2024* (5th ed.). https://www.itu.int/pub/D-HDB-GCI.01-2024

ISO/IEC. (2022). *Information security, cybersecurity and privacy protection—Information security management systems—Requirements* (ISO/IEC Standard No. 27001:2022). https://www.iso.org/standard/27001

Lawrence, P. R., & Lorsch, J. W. (1967). *Organization and environment: Managing differentiation and integration*. Division of Research, Graduate School of Business Administration, Harvard University.

Mollakuqe, E., & Dimitrova, V. (2024). Comparative analysis of identity management, access control, and authorization practices in public and private universities. *Open Research Europe, 4*, Article 23. https://doi.org/10.12688/openreseurope.16634.2

National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST SP 800-207). https://doi.org/10.6028/NIST.SP.800-207

National KE-CIRT/CC. (2024). *Cyber security report: January–March 2024* (33rd ed.). Communications Authority of Kenya.

Organisation for Economic Co-operation and Development. (2020). *The OECD digital government policy framework: Six dimensions of a digital government* (OECD Public Governance Policy Papers No. 2). OECD Publishing. https://doi.org/10.1787/f64fed2a-en

Parkinson, S., & Khan, S. (2023). A survey on empirical security analysis of access-control systems: A real-world perspective. *ACM Computing Surveys, 55*(6), Article 123. https://doi.org/10.1145/3533703

Peacock, R. (2025). Blind spots in Africa's cybersecurity strategies: Can policy and technology innovation mitigate the continent's systemic vulnerabilities? *Journal of Cyber Policy*. https://doi.org/10.1080/23738871.2025.2584826

Republic of Kenya. (2019). *The Data Protection Act, 2019*. Government Printer.

Verizon.(2024). *2024 data breach investigations report*.https://www.verizon.com/business/resources/reports/dbir/

World Bank. (2023, June 26). *From connectivity to services: Digital transformation in Africa*. https://www.worldbank.org/en/results/2023/06/26/from-connectivity-to-services-digital-transformation-in-africa

Yaokumah, W., &Okai, E. S. A. (2018). Inter-organizational study of access control security measures. *International Journal of Technology and Human Interaction, 14*(1), 60–79. https://doi.org/10.4018/IJTHI.2018010104