REVIEWED JOURNALS INTERNATIONAL
JOURNAL of Science & Technology
[ISSN 2663-127X]

Vol. 7, Iss. 1 (2026), pp 1 – 5, February 19, 2026. www.reviewedjournals.com, ©Reviewed Journals

CYBER SECURITY MEASURES AND PROTECTION OF PERSONAL DATA IN PUBLIC SECTOR INSTITUTIONS IN KENYA

[1] Stanley Kipkirui Koech & [2] Josphat Kyalo, PhD

[1] PhD Candidate, Kenyatta University, Kenya
[2] Lecturer, Management Science Department, Kenyatta University, Kenya

Accepted: February 3, 2026

ABSTRACT

In Kenya, government agencies face growing cyber-attack complexity as they quickly adopt digital systems for service delivery. Handling large amounts of sensitive data, such as biometric, financial, health, and identity info, increases their vulnerability. Kenya has enacted laws and policies like the Data Protection Act (2019) and the National Cyber security Strategy. Yet, government organizations find it hard to implement them. This paper reviews current cyber security practices in Kenyan public sector bodies. It evaluates the performance of government policies and laws. It also synthesizes recent research to find out how public institutions protect personal data. Based on existing policy papers, legal documents, institutional reports, and research papers, this study finds a gap between policy goals and actual practice. Despite relevant regulations, cyber security measures and their enforcement are underdeveloped and inconsistent, causing vulnerabilities and raising the risk of data breaches. The study suggests improvements to management and institutions to help grow cyber security and data protection in Kenya's public sector.

Key Words: *Cyber Security, Data Protection, Cyber-Attack*

CITATION: Koech, S. K., & Kyalo, J. (2026). Cyber Security Measures and Protection of Personal Data in Public Sector Institutions in Kenya. *Reviewed Journal of Science & Technology*, 7 (1), 1 – 5.

INTRODUCTION

In Kenya, the government now relies heavily on digital tech to deliver various services. Public offices use digital platforms for tasks such as managing ID systems, taxes, healthcare records, transportation, and citizen engagement (Government of Kenya, 2021). This shift has improved efficiency and broadened access to public services. On the flip side, it has also increased the vulnerability of these institutions to cyber-attacks, putting essential systems and large amounts of personal information at risk from rising cyber threats (Kinyua, 2024).Due to the nature of the information they manage, public institutions are attractive targets for cyber-attacks. Successful attacks on government systems can cause identity theft, loss of funds, service disruptions, and a decline in public trust (Saidi, Kimuyu, Handa, 2024). When key infrastructure like tax platforms or health databases are targeted, there can even be threats to national security and economic stability (Jonyo & Philip, 2024). As cyber threats become more sophisticated and frequent, the defense readiness of public institutions has become a central concern for governance and policy. To address these dangers, Kenya enacted the Data Protection Act (2019) and developed national cyber security plans aimed at protecting data and infrastructure (Government of Kenya, 2019; Government of Kenya, 2021). These policies establish standards for data handlers, promote accountability, and provide a framework for national cyber security. Yet, continued cyber incidents and compliance challenges suggest that policy creation has outpaced practical implementation within the public sector (Mathenge; Karani, 2024). This paper will examine the divide between policy and its application, studying the intersection of cyber security, government policies, and data protection in Kenya's public institutions.

THEORETICAL REVIEW

This study is guided by Institutional Cyber Security Governance Theory, which treats cyber security as a core governance function shaped by regulations, organizational skills, leadership engagement, and accountability frameworks (Taddeo, McCutcheon, &; Floridi, 2019; Linturi &; William, 2024). Current governance research finds that the success of cyber security depends on both formal rules and technical safeguards, as well as how well these are integrated into daily routines, managerial decisions, and accountability plans (Bada, Nurse, &; Sasse, 2020; Alshaikh, 2021).From this perspective, cyber vulnerabilities appear to be indicators of governance and organizational problems, not just technical concerns. Recent studies show that weak enforcement, flawed oversight, and underinvestment in personnel and cyber security training greatly undermine the use of cyber security practices, mostly in government sectors (ENISA, 2023; Mathenge &, Karani, 2024). Government organizations, which often face funding limits and complicated structures, are prone to governance-related cyber problems when leaders show inconsistent support and departments do not collaborate well (Jonyo &; Philip, 2024; Ogutu, Obosi, &; Odongo, 2025).

METHODOLOGY

This research uses a thematic content analysis. Information is gathered from Kenyan laws and national policies, like the Data Protection Act (2019) and the National Cyber security Strategy (2022–2027). These form the legal and strategic support for cyber security and data protection in Kenya's government (Government of Kenya, 2019; Government of Kenya, 2021). Additional information comes from government and regulatory reports on policy implementation, institutional guidelines, audit reports on organizational practices, and academic articles that assess cyber governance issues in Kenya and the region (Mathenge &; Karani, 2024; Kinyua, 2024; Sema, Owolawi, &; Olugbara, 2025).Thematic document analysis was employed to identify themes about cyber security measures, policy action problems, and personal data protection within government groups. This type of analysis is a standard way to gather information from regulatory texts and institutional reports in cyber governance studies, showing links between policy and real-world practice (Kaifa, Yaseen, &; Muzaffar, 2025). Through repeated coding and grouping of documents, this method aided in finding governance gaps, enforcement inconsistencies, and differences in how Kenyan organizations handle cyber security and data protection.

FINDINGS

Cyber Security Measures

Most research indicates that Kenyan public sector entities implement basic cyber security, such as firewalls, antivirus software, and access controls, largely to adhere to national standards (Kinyua, 2024; Mathenge &; Karani, 2024). Similarly, Ogutu, Obosi, and Odongo (2025) observed that cyber security adoption in Kenyan public entities is compliance-driven rather than risk-management-driven.

Kenya's approach is typical compared to its African peers. Sema, Owolawi, and Olugbara (2025) noted that South African public entities prioritize adherence to cyber regulations but lack capabilities in detection and response. Adeyemi et al. (2025) reported that West African public entities tend to concentrate on basic security technologies while neglecting continuous monitoring and incident planning.

Conversely, countries with sophisticated digital public sectors manage cyber security differently. Studies in Europe and developed nations suggest the adoption of risk-based cyber security models, which include technologies like intrusion detection systems and incident response strategies (ENISA, 2023; Alshaikh, 2021). These studies suggest that executive leaders consider cyber security integral to organizational management.

Organizational structure is another point of divergence. Research within Kenya suggests that cyber security is typically a function of IT departments, which constrains strategic planning (Kinyua, 2024; Jonyo &; Philip, 2024). Similar arrangements exist in other African nations (Adeyemi et al., 2025). Global research suggests assigning dedicated cyber security teams, such as those led by Chief Information Security Officers, can contribute to increased security and accountability (Taddeo, McCutcheon, &a; Floridi, 2019; ENISA, 2023).In summary, Kenyan public entities implement basic cyber security similar to other African nations, but lag behind global leaders. The latter emphasize early threat detection, risk assessment, and integrating security into their strategic initiatives. Experts suggest that, as cyber threats become increasingly sophisticated, merely meeting minimum security standards exposes public entities to increased vulnerability. They stress the need to transition from a compliance-oriented approach to building security strategies driven by executive leadership (Ogutu et al., 2025; Sema et al., 2025).

Cyber Security Measures and Legal Implication

The Data Protection Act (2019) is generally considered a progressive legal framework that aligns Kenya’s data protection system with global standards. Several authors note the Act’s solid basis, such as its embrace of principles like accountability, data minimization, lawful processing, purpose limitation, and the establishment of proper technical and organizational safeguards (Mathenge &; Karani, 2024; Sema, Owolawi, & Olugbara, 2025). Some analysts argue that Kenya’s law compares favorably with established international systems like the European Union’s General Data Protection Regulation (GDPR), at least in terms of structure and the expression of rights (Kinyua, 2024).

While there's a consensus on the strength of the legal structure, opinions diverge about the degree of institutional compliance and the outcomes of its implementation. For instance, Mathenge and Karani (2024) take a legal perspective, suggesting that the Act’s major issue is in its execution, citing weak enforcement mechanisms and a lack of integration within public sector bodies. Conversely, Ogutu, Obosi, and Odongo (2025), using an institutional capacity analysis, place emphasis on human and organizational issues. They claim that public officials' lack of awareness and insufficient technical skills greatly impede compliance.

Other analysts take a governance-based approach to discuss problems with the enforcement structure. Kinyua (2024) observes that while compliance structures like data registers and consent systems are becoming more common in public bodies, they're often superficial, mainly intended to show compliance rather than genuinely protect data. This contrasts with Jonyo and Philip’s (2024) assertion that poor enforcement is worsened by divided oversight and poor coordination among agencies, especially between sector regulators and the Office of the Data Protection Commissioner.

Comparative studies clarify this difference. Sema et al. (2025), in their study of South Africa's Protection of Personal Information Act (POPIA), state that while South Africa has similar compliance issues, stronger enforcement tools—like mandatory compliance reporting and more frequent regulatory audits—have produced greater institutional knowledge than in Kenya. By contrast, Adeyemi et al. (2025) find that in certain West African areas, data protection laws exist mainly on paper due to very limited enforcement capacity, positioning Kenya somewhere between mere adoption and practical implementation.

Overall, while analysts consistently state that the Data Protection Act (2019) is legally sound and in line with international standards, they offer different explanations for its apparent inability to prevent wrong behavior in practice. Legal experts tend to focus on gaps in the enforcement structure, institutional researchers cite inadequate skills and capacity, and governance-centered studies point to divided accountability and oversight structures. This variation points to a key idea: that sound data protection in the public sector depends less on complex laws and more on the combined of enforcement capacity, institutional readiness, and governance (Ogutu et al., 2025; Sema et al., 2025).

Kenya's National Cyber security Strategy is regarded as a solid policy that aligns national cyber security objectives with global standards, particularly in risk management, collaboration, and capacity building (Government of Kenya, 2021; Linturi &; William, 2024). Its concepts are well-received, but research indicates practical challenges within the government.

Observed problems include skill gaps, funding shortages, and a lack of dedicated cyber security units to execute strategies (Mathenge &; Karani, 2024; Kinyua, 2024). Insufficient cyber security training and limited learning opportunities complicate threat data sharing and incident response (Ogutu et al., 2025).

Coordination and management issues, such as task duplication and unclear roles, impede collaboration among groups (Jonyo &; Philip, 2024). Studies in other African nations suggest policy implementation lags, unlike Europe, where stable funding and strong agencies support plan execution (Sema et al., 2025; ENISA, 2023).

Overall, research suggests that Kenya's National Cyber security Strategy, while providing sound guidance, faces difficulties due to leadership, resource, and skill deficits. This suggests a need for practical adjustments to improve the government's cyber security defenses.

Scholars generally agree that data protection in Kenya's public sector differs depending on where it is in its lifespan. This mirrors more general governance and capability concerns. Research indicates that while institutions are starting to use compliance tools like data registers after the 2019 Data Protection Act, the actual controls they use are either weak or not consistently followed. These studies suggest that current rules emphasize documentation over real risk handling, which causes issues like data classification and safe disposal to be overlooked.

In general, researchers concur that issues in data handling, retention, disposal, and third-party management suggest basic governance deficits, not only tech issues. Even though Kenya's legal base is strong, research shows that institutions need to change. These changes should include data protection in how groups are run, instead of seeing it as just another compliance task.

The study underscores the policy practice gap in Kenya's public sector. Despite existence of cyber security and data protection polices, the limited resources, professionals in the field, weak management system as well as ineffective enforcement all militate against their implementation. This means we must start to think about cyber security as a governance problem, and not purely a technical one.

DISCUSSION CONCLUSION AND RECOMMENDATION

Research indicates an alignment globally: deficient management hinders strong cyber security in governmental organizations. The Kenyan example shows that regulations alone do not assure data safety.

Without sustained commitment to skill enhancement, rule adherence, and responsible leadership, cyber security strategies may prove inadequate. The increasing reliance on digital systems inside government amplifies the risk to institutions and citizens rooted in these essential deficiencies.

Kenya has advanced in creating cyber security and data protection policies. This study, though, shows that implementing these policies is still hard for public organizations. To address the gap between policy and practice, governance reforms, sustained investment in training, and better ways to enforce rules are necessary. Strengthening cyber security in the public sector is key to protecting data and preserving public confidence in Kenya's digital government initiatives.

To boost cyber security, this paper proposes a detailed plan that strengthens regulations and organizational structures. It suggests increased oversight through greater funding for regulatory bodies, enhancing their auditing skills and compliance enforcement. The plan also calls for stronger cyber security management by establishing specialized teams led by senior staff. It emphasizes the requirement for improved personnel skills through regular training and certifications to handle changing threats. Adopting better security tech, like advanced threat detection and continuous monitoring systems, is important for locating and addressing problems. The paper concludes that teamwork is vital, advocating for partnerships to strengthen a country's cyber defenses.

REFERENCES

Government of Kenya. (2019). *Data Protection Act*. Nairobi: Government Printer.

Government of Kenya. (2021). *National Cybersecurity Strategy 2021–2025*. Nairobi: Ministry of ICT.

Jonyo, F., & Philip, K. (2024). Public–private partnerships and cyber security governance in Kenya. *National Security Journal*, 7(1), 45–62.

Kinyua, C. G. (2024). Cybersecurity risks in Kenyan government institutions. *Journal of Environmental Sustainability Advancement Research*, 3(2), 88–102.

Linturi, T., & William, C. N. (2024). Adaptive cyber resilience policies in public sector institutions. *National Security Journal*, 7(2), 63–79.

Mathenge, R., & Karani, J. (2024). Legal frameworks for digital space protection in Kenya. *International Journal of Computer and Information Technology*, 13(4), 112–125.

Alshaikh, M. (2021). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003.

Bada, M., Nurse, J. R. C., & Sasse, M. A. (2020). Cyber security awareness campaigns: Why do they fail to change behaviour? *Information & Computer Security*, 28(1), 71–85.

ENISA. (2023). *Cybersecurity governance guidelines for public administrations*. European Union Agency for Cybersecurity.

Kaifa, U., Yaseen, D. Z., & Muzaffar, D. M. (2025). A thematic analysis of cybersecurity policies, regulations and implications. *Journal of Climate and Community Development*, 4(1), 39–54.

Ogutu, K. O., Obosi, J. O., & Odongo, H. A. (2025). Cybersecurity training and institutional capacity in Kenya. *Journal of Public Policy and Administration*, 9(1), 21–38.

Saidi, I. C., Kimuyu, J. J., & Handa, S. (2024). Cybercrime and economic security in Kenya. *International Journal of Research and Innovation in Social Science*, 8(3), 134–149.

Sema, G. G., Owolawi, P. A., & Olugbara, O. O. (2025). Data protection law implementation in African public institutions. *Sustainability*, 17(2), 1–15.