Journal of Information Systems and Informatics
Vol. 7, No. 2, June 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i2.1100 Published By DRPM-UBD

# Data Protection and Cybersecurity in E-Waste Disposal: Evidence from Tanzania's Public Institutions

**Athuman Mustapha[1], Bonny Mgawe[2], Jaha Mvula[3], Anael Sam[4]**

[1,2]Nelson Mandela African Institution of Science and Technology; Tanzania
[3]Electronic Government Authority (eGA); Tanzania
[4]Nelson Mandela African Institution of Science and Technology; Tanzania
Email: [1]mustaphaa@nm-aist.ac.tz, [2]bonny.mgawe@nm-aist.ac.tz, [3]jaha.mvula@ega.go.tz, [4]anael.sam@nm-aist.ac.tz

**Abstract**

The growing volume of electronic waste (e-waste) in Tanzanian public institutions poses serious cybersecurity risks, as discarded devices often contain sensitive data vulnerable to unauthorized access. This study examines these risks across 11 public institutions, involving IT staff, e-waste handlers, policymakers, and environmental officers. It applies Routine Activity Theory, a framework that explains risks as arising when cybercriminals exploit unsecured e-waste due to weak regulations. Through interviews and focus group discussions, the research identifies key vulnerabilities: data leakage from improper sanitization, regulatory gaps, and risks from informal disposal methods like auctions. These findings highlight the need for stronger oversight to prevent data breaches. The study proposes a framework that categorizes devices by risk level and integrates secure sanitization protocols, such as data wiping or destruction. Policymakers and institutions must urgently adopt these protocols to protect sensitive data and promote sustainable e-waste management in Tanzania's public sector.

**Keywords**: cybersecurity, e-waste disposal, Routine Activity Theory, data leakage, institutional oversight, Tanzania.

## 1. INTRODUCTION

The rapid increase in the use of electronic devices in public institutions—including smartphones, laptops, and storage media—has led to a significant rise in electronic waste (e-waste). E-waste refers to discarded electrical and electronic equipment (EEE) [1], which has become a pressing global issue. In 2022, global e-waste reached an alarming 62 million tons, and it is projected to grow to 82 million tons by 2030. Africa, in particular, faces a dual challenge, generating 50–85% of its e-waste domestically while also being a major destination for illegal e-waste imports [2]. In Tanzania's public institutions, improper e-waste disposal introduces significant cybersecurity risks, as sensitive data stored on discarded devices can be recovered and misused, leading to data breaches, fraud, and even potential national security threats [3].

Despite the growing global focus on e-waste, there is a critical gap in addressing the cybersecurity risks that e-waste poses within Tanzania's public sector. Regulatory frameworks often prioritize environmental concerns over data security [4], leaving public institutions vulnerable to the exploitation of discarded electronic devices. Sensitive data, such as financial records, personal identification information, and confidential communications, may be exposed if the internal memory of discarded devices is not properly wiped or erased. If these devices are resold, recycled, or disposed of without securing the data, it could lead to fraud, identity theft, and threats to national security [5].

While e-waste disposal is typically considered an environmental issue, it poses a significant cybersecurity threat that affects not only public institutions but also private organizations and individuals. With the vast amount of sensitive information—such as contact details, emails, banking information, photographs, and videos—stored on ICT devices, the risk of data misuse upon improper disposal is substantial. As highlighted by [6], a key concern is the lack of standardized procedures to address the cybersecurity risks that arise from e-waste disposal in these institutions. Forgor et al. [7] further emphasize the alarming reality that even after basic formatting procedures, residual data can still be easily retrieved using simple data recovery software. This leaves sensitive information vulnerable to recovery by individuals with malicious intent, such as cybercriminals or unauthorized third parties, raising serious concerns about the security of personal, organizational, and national data.

In Tanzania's public institutions, the issue is exacerbated by weak regulatory enforcement and informal disposal practices, including auctions, a culture of discarding devices without proper consideration, leaving devices in office rooms, and donating old equipment without adequate data sanitization. These practices create an environment ripe for data leakage. Routine Activity Theory (RAT) offers a framework to understand these risks, where the convergence of three factors—motivated offenders (cybercriminals), suitable targets (unsecured e-waste), and the absence of capable guardians (inadequate policies and practices)—results in significant vulnerabilities.

This study aims to investigate the cybersecurity risks linked to e-waste disposal practices in Tanzania's public institutions, focusing on three key research questions: (1) What are the current e-waste disposal practices in Tanzanian public institutions, and how do they contribute to cybersecurity vulnerabilities? (2) What regulatory gaps exist in managing e-waste securely? (3) What measures can be implemented to mitigate these risks effectively? The study's objectives are to assess current e-waste disposal practices, identify vulnerabilities, and propose a secure disposal framework through standardized sanitization protocols.

By addressing this research gap, the study not only contributes to a deeper understanding of Tanzania-specific e-waste cybersecurity risks but also adds to the global dialogue on secure disposal practices. The proposed framework will be tailored to the unique needs of Tanzania's public sector, aligning cybersecurity with sustainable IT asset management. Ultimately, this research aims to inform policy reforms that will safeguard sensitive data, promote secure e-waste disposal, and encourage the adoption of circular economy principles in Tanzania's public institutions.

## 2. Related Works

### 2.1. Theoretical Framework

Routine Activities Theory (RAT) is a criminological framework that explains how crime occurs when three critical elements converge in time and space: a motivated offender, a suitable target, and the absence of a capable guardian [8]. This theory can be effectively applied to understanding the cybersecurity risks associated with e-waste disposal. In the context of e-waste, RAT highlights how the lack of proper data disposal procedures creates an environment ripe for exploitation by cybercriminals. The three key elements of RAT in relation to e-waste are:

1) Motivated Offender: Cybercriminals or malicious actors who actively seek to exploit improperly disposed e-waste devices in order to steal sensitive data.
2) Suitable Target: Discarded e-waste containing unsecured data, such as hard drives, laptops, smartphones, and other storage devices, which can serve as prime targets for data extraction.
3) Absence of a Capable Guardian: The lack of effective regulations, policies, or practices to ensure secure disposal of e-waste, allowing cybercriminals to exploit the vulnerable devices without significant deterrence.

This study adopts RAT to examine how the absence of capable guardians—such as inadequate regulatory frameworks or the absence of proper data sanitization protocols creates opportunities for cybercriminals to exploit vulnerable e-waste. The proposed framework in this study aims to reduce these cybersecurity risks by introducing standardized sanitization procedures and enhancing policies to secure the disposal process.

Numerous researchers have examined the broader societal and environmental impacts of e-waste. However, there has been a notable lack of focus on the specific cybersecurity implications of e-waste management. While government regulations often focus on environmental concerns, the risks to data security remain an overlooked issue. Alghazo et al.'s research in the Gulf Cooperation Council (GCC)

highlights the general public's ignorance about data security risks, particularly the misconception that once data is deleted or formatted from a device, it is irretrievable [9]. This misunderstanding contributes to a lack of proper data disposal practices, leaving sensitive information vulnerable to recovery. Additionally, Balde et al. [10] assert that government and financial organizations are especially prone to cybersecurity vulnerabilities due to flaws in their policies and procedural guidelines. These sectors, which handle vast amounts of sensitive information, are at heightened risk if their e-waste disposal practices are not adequately secured.

### 2.2. Global and Regional E-Waste Assessment

A comprehensive analysis of the global e-waste situation is provided by the Global E-Waste Monitor 2024, which underscores the magnitude of the issue on a global scale [11]. This report highlights the rapid growth of e-waste and its environmental implications, while also shedding light on the complex challenges faced by various regions in managing e-waste. For example, while e-waste is a global problem, its management varies significantly by region, influenced by local economic, regulatory, and technological factors.

In particular, Tanzania has faced considerable difficulties in managing e-waste effectively, as highlighted by regional studies [12]. Similarly, broader regional studies on Africa [13] illustrate the unique challenges that the continent faces in dealing with e-waste, including limited infrastructure, inadequate regulations, and the influx of illegal e-waste imports. These challenges make it difficult to manage e-waste securely, especially in the context of cybersecurity risks, which are often neglected in favor of environmental concerns.

### 2.3. Cybersecurity Implications of E-Waste

The improper disposal of e-waste can pose severe cybersecurity risks, a concern emphasized in studies such as that by K. Daum et al., which focused on the export of e-waste to countries like Ghana [14]. Devices such as laptops, smartphones, and hard drives, when discarded without proper data sanitization, can easily be scavenged for leftover data. Cybercriminals can exploit this unsecured data using widely available recovery tools, thereby compromising sensitive personal or organizational information.

This highlights the critical need for secure data sanitization practices in e-waste disposal. Without these measures, discarded devices become ideal targets for cybercriminals looking to exploit vulnerabilities in the disposal process. This issue is particularly pressing for public institutions, where sensitive government and national security data may be at risk if proper disposal practices are not in place.

### 2.4. Forensic Analysis and Data Extraction

Forensic studies have demonstrated that data can often be recovered from abandoned electronic devices, even if they are believed to have been "wiped." Szewczyk et al. [16] found that a large percentage of readable USB storage devices, 95% in their analysis, contained retrievable data. This demonstrates the shortcomings of basic data disposal techniques, such as simple formatting or deletion, which fail to thoroughly erase sensitive information. These findings emphasize the importance of adopting more comprehensive data disposal techniques that go beyond basic formatting procedures. Such techniques must ensure that all residual data is fully destroyed before devices are discarded, recycled, or repurposed. Failure to do so leaves the door open for cybercriminals to retrieve sensitive information, even from devices that have been seemingly "wiped clean."

### 2.5. Data Security Threats and Data Management

Organizations and external vendors responsible for managing e-waste must comply with stringent data privacy regulations and secure data handling practices. However, as pointed out by Ichikowitz et al. [18], secure data handling often falters when devices reach the end of their lifecycle (EOL). The rapid growth of e-waste now outpaces advancements in disposal technologies, resulting in residual data on outdated devices that remains vulnerable to exploitation.

The emergence of mobile workforces and the increasing adoption of Bring Your Own Device (BYOD) policies have further compounded this issue. These trends, while enhancing workplace flexibility, increase the reliance on personal ICT devices that may not always meet the same security standards as organizational equipment. Alqahtani et al. [21] and Escobar-Rodríguez et al. [22] caution that such practices expose organizations to significant data security vulnerabilities, especially when users overestimate the security of their personal devices.

As cybercriminals continue to target e-waste disposal networks to harvest sensitive data, it is essential for both the public and private sectors to implement strict data privacy safeguards throughout the e-waste lifecycle. Non-compliant disposal practices can leave sensitive personal identifiable information (PII) exposed to unauthorized access, fraud, identity theft, and other forms of exploitation [23].

In conclusion, the cybersecurity implications of e-waste disposal are significant and demand immediate attention. As highlighted by the studies reviewed in this section, securing the disposal process is critical to preventing unauthorized access to sensitive data. Therefore, it is crucial to adopt comprehensive data sanitization practices and ensure that e-waste disposal policies are in line with international

standards and best practices. The evolving nature of cyber threats requires continuous updates to data security protocols to safeguard against exploitation in the rapidly growing e-waste environment.

## 3. METHODOLOGY

This study adopts a qualitative methodology to investigate e-waste disposal practices and associated cybersecurity risks in Tanzanian public institutions, aligning with the research purpose of identifying vulnerabilities and proposing a secure disposal framework. The methods, grounded in a constructivist paradigm, emphasize participants' subjective experiences to uncover nuanced insights into institutional practices.

### 3.1. Philosophical paradigm and research strategy

The study employs an inductive thematic analysis to explore the complexities of e-waste disposal and cybersecurity risks, guided by a constructivist paradigm that values participants' diverse perspectives [24]. This approach ensures findings, such as themes like "Throw away" and "Donation as way to dispose," emerge directly from participants' narratives. A case study strategy contextualizes these phenomena within Tanzanian public institutions, using semi-structured interviews and focus group discussions (FGDs) to capture individual and collective insights, respectively.

### 3.2. Sampling

A purposive sampling strategy was used to select participants with expertise relevant to e-waste disposal and cybersecurity, prioritizing depth over generalizability [25]. Eleven public institutions, spanning ministries, regulatory bodies, and public service organizations, were chosen to represent diverse sectors of Tanzania's public sector, ensuring a comprehensive view of e-waste practices. Within these institutions, participants were selected based on specific roles to ensure diversity and relevance: IT/information security personnel (5) for data security expertise, e-waste disposal officers (3) for practical disposal knowledge, administrators/policy enforcers (2) for regulatory insights, and an environmental officer (1) for sustainability perspectives. These roles were chosen to cover the e-waste management lifecycle, from policy to execution, and to reflect varied institutional functions. The sample size of 11 institutions was determined by data saturation, where no new themes emerged, validating the findings' robustness [26].

### 3.3. Data collection instruments

Data were collected through semi-structured interviews and one FGD. Interviews, conducted one-on-one, used a guide with questions like, "What procedures does your institution follow for e-waste disposal?" and "Have you encountered data breaches from improper disposal?" The FGD, with 6 participants, fostered discussion on shared challenges and solutions. The interview and FGD guide is provided in **Appendix A**. To minimize researcher bias during data collection, interviewers used neutral phrasing, avoided leading questions, and allowed participants to elaborate freely. All sessions were audio-recorded with consent and transcribed verbatim.

### 3.4. Qualitative Analysis Process

The analysis followed Braun and Clarke's thematic analysis framework [27], conducted by three researchers to enhance reliability and reduce bias. The process included five steps:

1) Data Familiarization: Researchers independently reviewed transcripts three times, noting initial patterns to immerse themselves in the data.
2) Initial Coding: Using ATLAS.ti version 24, codes were generated inductively from the data. Specific settings included open coding with no predefined categories, and memos were used to document coding rationales.
3) Theme Development: Codes were grouped into candidate themes using ATLAS.ti's network visualization tools, which mapped code relationships to ensure coherence.
4) Review and Refinement: Themes were validated against raw data, with discrepancies resolved through consensus discussions to mitigate individual researcher bias.
5) Interpretation: Themes were interpreted through Routine Activity Theory (RAT), linking regulatory gaps (absent guardians) to cybersecurity risks.

ATLAS.ti version 24's query tools and code co-occurrence functions supported systematic analysis, ensuring reproducibility. Collaborative coding and regular team meetings further minimized bias by cross-checking interpretations.

### 3.5. Ethical Considerations

Ethical integrity was maintained through informed consent, where participants received detailed study information and provided written consent, with the option to withdraw. Confidentiality was ensured by anonymizing data with pseudonyms (Participant1, Participant2, etc.) and storing transcripts securely, accessible only to the research team.

### 3.6. Ensuring Consistency

Reliability and validity were enhanced through triangulation, cross-verifying data from interviews, FGDs, and literature. Member checking involved sharing preliminary findings with four participants to confirm accuracy. An audit trail documented coding decisions and theme revisions, supporting transparency.

## 4. RESULTS AND DISCUSSION

This study investigates e-waste disposal practices within Tanzanian public institutions, focusing on the associated cybersecurity vulnerabilities. As the improper disposal of electronic waste (e-waste) continues to pose significant threats to data security, it is essential to understand the specific practices and challenges faced by public institutions in Tanzania. To achieve this, a comprehensive qualitative analysis was conducted, incorporating interviews with key stakeholders from various public institutions, as well as focus group discussions. These discussions were designed to capture a broad range of insights from individuals directly involved in or impacted by e-waste disposal processes, including IT staff, administrators, and policy experts.

The qualitative research methodology enabled the study to delve deep into the nuances of current e-waste disposal practices, uncovering not only the practical realities of how devices are handled but also the broader organizational and regulatory factors that influence these practices. The study aimed to capture both the observable practices and the underlying reasons for these practices, particularly as they relate to cybersecurity concerns.

The findings from the interviews and focus groups revealed several critical themes, which have been organized into distinct categories to better understand the challenges and risks present in Tanzania's public sector e-waste disposal practices. These themes provide insight into the relationship between disposal methods, regulatory gaps, and the security risks associated with improper handling of electronic devices. For instance, one prominent theme that emerged was the widespread lack of awareness about the security implications of e-waste. Many stakeholders expressed a limited understanding of how improperly disposed devices, if not properly sanitized, could lead to significant data breaches, fraud, or even threats to national security.

### 4.1. Regulatory framework overview

The regulatory framework governing e-waste disposal emerged as a central theme, characterized by a lack of cohesive policies addressing cybersecurity. Participants

frequently noted that existing regulations, such as Regulation 51 of the Environmental Management Act, focus primarily on environmental protection rather than data security. For instance, a participant from a regulatory body explained, "We follow environmental laws for disposal, but there's nothing specific about protecting data on these devices." This gap leaves institutions vulnerable to breaches, as sensitive information on discarded devices remains accessible. The ad hoc network in Figure 1 illustrates how participants perceive these regulations, with nodes connecting environmental, financial, and general regulations, yet highlighting the absence of cybersecurity-focused policies.

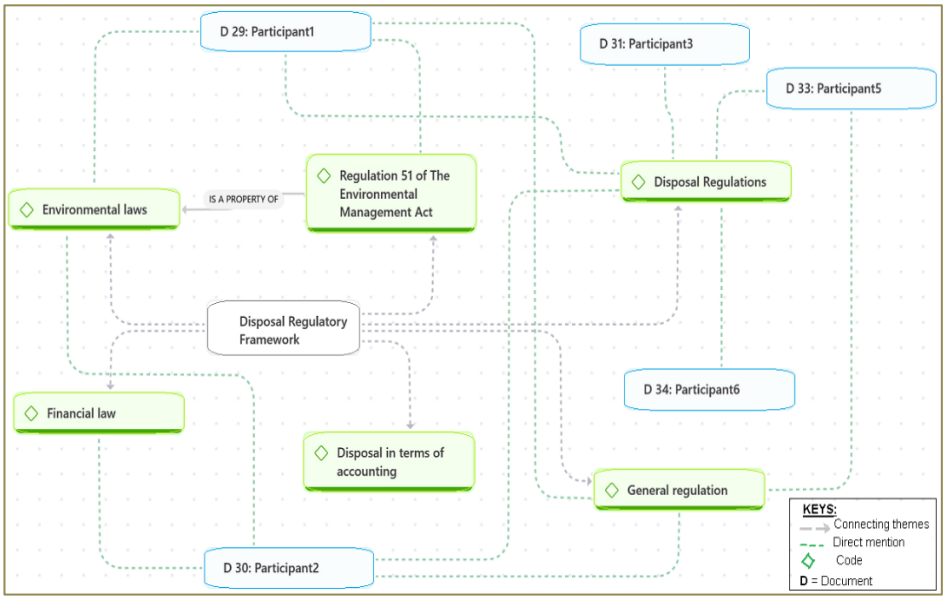


**Figure 1**. The Ad hoc network of disposal regulatory framework theme

### 4.2. Implementation of e-waste regulations

Further exploration revealed that the implementation of e-waste regulations is inconsistent across institutions. A participant (Participant5 on D33) shared, "At the organizational level there is no specific policy or regulation that govern e-waste disposal" "There's a 2022 regulation for electronic communication equipment, but it doesn't guide us on securing data during disposal." continued the participant. Another Participant7 (D35) emphasized, "At our organization, we lack formal procedures for e-waste management." These insights, visualized in Figure 2, underscore a fragmented regulatory landscape where guidelines are either absent or insufficiently enforced, exacerbating cybersecurity risks. The lack of oversight creates opportunities for improper handling of data-bearing devices, aligning with Routine Activity Theory's concept of absent guardianship.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

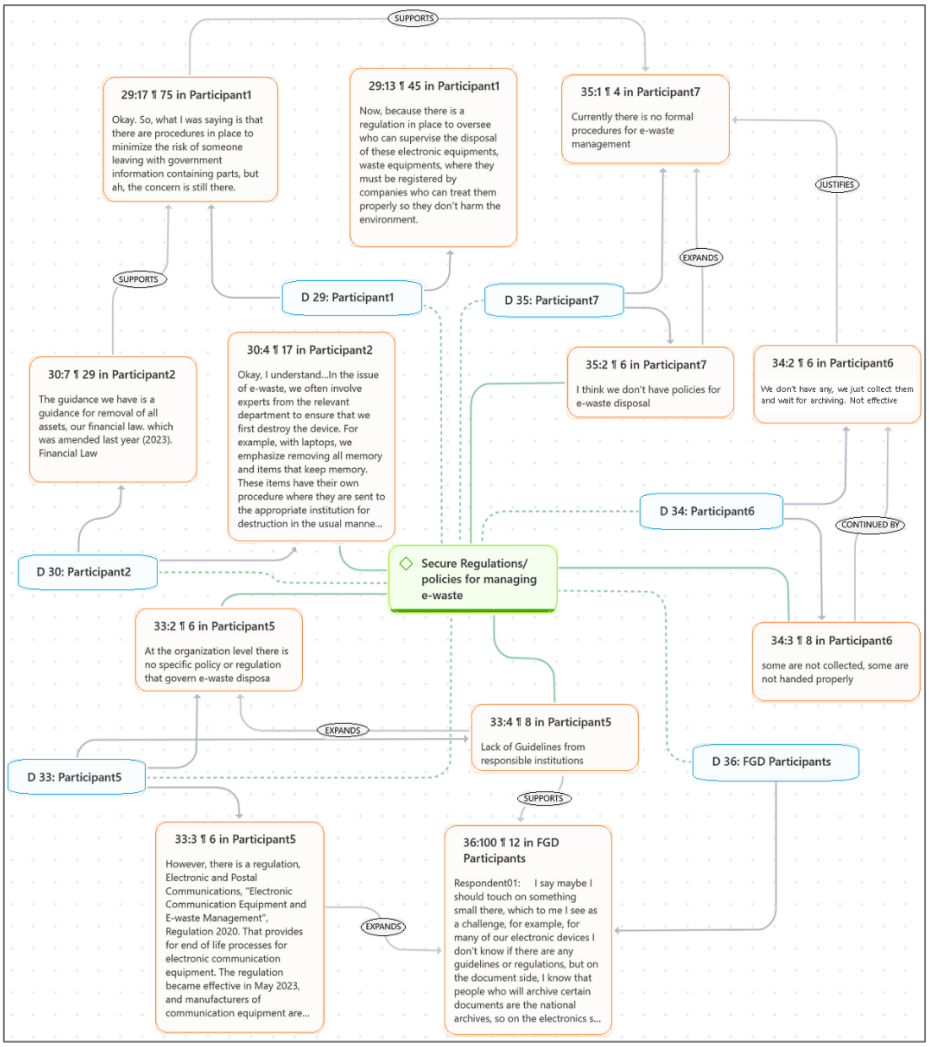


**Figure 2.** Participant's insights on regulations/policies for managing e-waste disposal

### 4.3. E-waste disposal practices

The study identified diverse disposal practices, many of which are insecure and unregulated. Participants described methods such as auctions, donations, and informal discarding, often without data sanitization. Participant1 noted, "We either auction or donate old computers" Similarly, another Participant2 admitted, "Some departments just throw away devices because there's no clear protocol." The ad hoc network in Figure 3 captures these practices, revealing a lack of standardization

that heightens the risk of data leakage. These findings indicate that unclear procedures directly contribute to cybersecurity vulnerabilities.

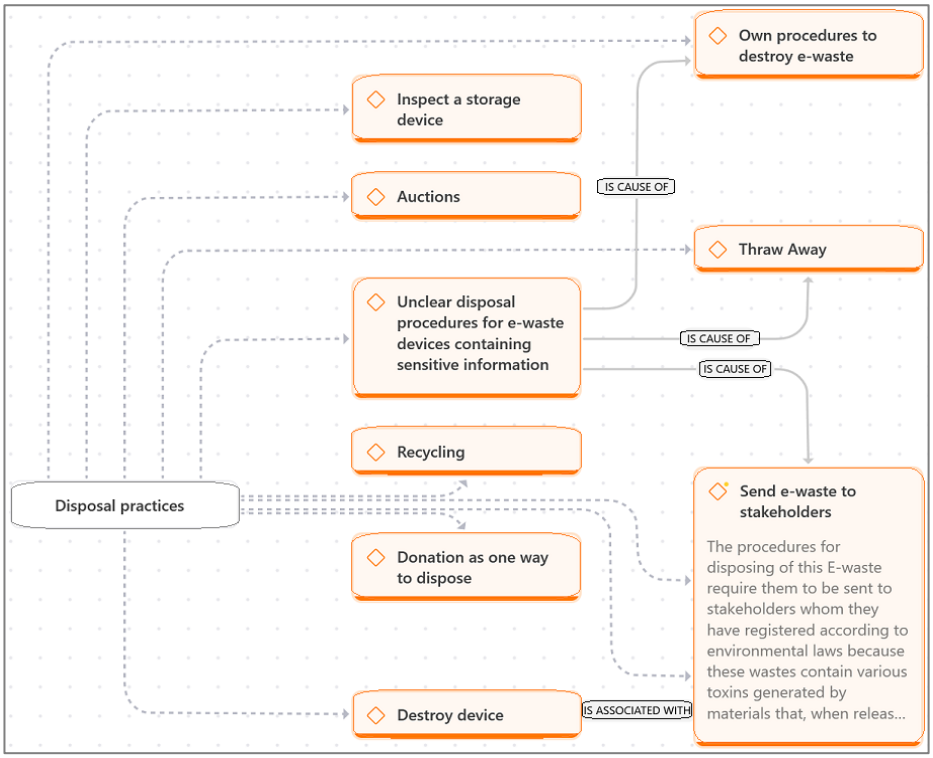


**Figure 3**. The Ad hoc network of disposal practices

Furthermore, the node "Unclear disposal procedure for e-waste devices that contain sensitive information" is closely tied to several other practices, each reflecting a potential consequence of inadequate guidance on secure disposal:

1) Own procedures to destroy e-waste – in the absence of clear, standardized protocols, institutions might develop their own methods to destroy e-waste. While well-intentioned, these ad hoc approaches may not sufficiently secure the sensitive information stored on these devices, leaving data vulnerable to unauthorized access.
2) Send e-waste to stakeholders – when institutions send e-waste to external stakeholders for disposal or recycling, the lack of clear procedures can lead to inconsistent handling of sensitive data. Without explicit instructions, stakeholders may fail to adequately safeguard this information, increasing the risk of data breaches.
3) Throw away – this represents the most concerning outcome of unclear procedures; careless disposal. When e-waste is simply discarded without

proper attention to data security, it can lead to significant cybersecurity threats, as sensitive information remains accessible.

4) Recycling – even in recycling processes, the lack of clear disposal instructions can result in sensitive data being inadequately erased from devices, leaving them vulnerable to recovery and misuse.

Again, these connections emphasize the critical need for well-defined, enforceable disposal procedures that prioritize the secure handling of sensitive information throughout the e-waste disposal process.

### 4.4. Cybersecurity vulnerabilities

Participants consistently highlighted cybersecurity risks stemming from improper disposal. A participant in FGD recounted, "We found discarded hard drives with recoverable data, which could have been a major breach." Another Participant6 expressed concern, stating, "Without oversight, sensitive information can easily fall into the wrong hands." These vulnerabilities, depicted in Figure 4, align with Routine Activity Theory, where the absence of capable guardians (regulations and protocols) enables motivated offenders (cybercriminals) to exploit suitable targets (unsecured e-waste). The findings emphasize the urgent need for secure disposal practices to protect institutional data.

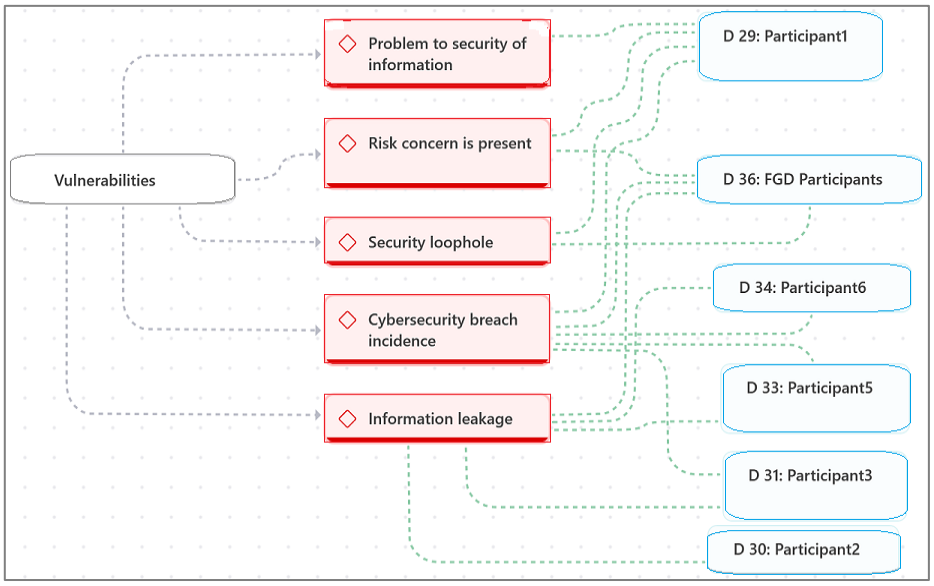


**Figure 4**. The network of nodes showing participant's experience on the effects of current disposal practices

To provide a clear overview, Table 1 summarizes the key themes and subthemes identified in the analysis, offering a concise reference for the complex interplay of regulatory, practical, and security issues.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

**Table 1.** Summary of Key Themes and Subthemes

| Theme | Subthemes |
|---|---|
| Regulatory Framework | Environmental focus over cybersecurity, lack of cohesive policies |
| Existing Regulations | Fragmented and inadequate for data security, absence of formal procedures |
| Disposal Practices | Inconsistent methods (auctions, donations), lack of standardization |
| Cybersecurity Vulnerabilities | Data leakage risks, security breach incidents, absence of oversight |

### 4.5. Discussion

The findings from this study paint a vivid picture of the cybersecurity challenges embedded in Tanzanian public institutions' e-waste disposal practices. By breaking down the results into regulatory, practical, and vulnerability-focused themes, the discussion connects these insights to broader research and proposes actionable solutions through the lens of Routine Activity Theory (RAT).

The regulatory framework, as participants described, is heavily skewed toward environmental and financial compliance, with little attention to cybersecurity. This mirrors findings from other African contexts, such as Ghana [28], where e-waste regulations prioritize waste management over data protection, leading to data breaches in informal markets. The Tanzanian context, however, faces unique challenges due to limited resources and awareness, as one participant noted: "We don't have the knowledge regarding data security on e-waste." This gap underscores the need for Tanzania-specific policies that balance environmental and security imperatives.

Disposal practices in Tanzanian institutions, characterized by auctions, throw away, and donations without standardized protocols, exacerbate cybersecurity risks. Participants' accounts, such as "We auction or donate old computers", highlight a systemic issue also observed in South Africa, where informal disposal has led to data recovery from second-hand devices [19]. Unlike the Gulf Cooperation Council countries, where higher awareness of data security informs disposal practices [29], Tanzania's public sector lacks such prioritization. This comparison suggests that capacity-building and regulatory enforcement could bridge this gap, aligning local practices with global standards.
The identified cybersecurity vulnerabilities, including data leakage and potential breaches, resonate with global concerns about e-waste as a security threat. For instance, studies in Australia have shown that 95% of discarded storage devices contain recoverable data [16], a risk echoed in Tanzania's context where oversight

is minimal. The participant's warning, "Sensitive information can easily fall into the wrong hands," aligns with Routine Activity Theory's premise that weak guardianship enables exploitation. Unlike developed nations with robust sanitization guidelines, Tanzania's public institutions face resource constraints, necessitating tailored solutions like the proposed framework.

The Secure E-Waste Disposal Framework developed in this study (Figure 6) addresses these challenges by categorizing devices based on data sensitivity and functionality, ensuring appropriate sanitization methods; clearing, purging, or destruction. This approach draws inspiration from NIST guidelines in the United States, which advocate risk-based disposal, but adapts them to Tanzania's resource-limited context. By institutionalizing capable guardianship through standardized protocols, the framework reduces the suitability of e-waste as a target for cybercriminals, offering a practical and theoretically grounded solution. Policymakers in Tanzania should prioritize its implementation to safeguard institutional data and contribute to sustainable e-waste management.

### 4.5.1. The frame for secure disposal practices

The developed framework in **Figure 6** addresses the vulnerabilities identified by participants through the three elements of RAT by institutionalizing capable guardianship and reducing the suitability of e-waste as a target for cybercriminals:

1) Capable Guardian: The framework establishes robust protocols for data sanitization, device categorization, and disposal validation, acting as a guardian to prevent unauthorized access to sensitive data.
2) Suitable target: In categorizing devices based on data sensitivity and functionality, the framework reduces the attractiveness of e-waste (especially those containing highly sensitive information) as a target since they are destroyed, making data recovery nearly impossible.
3) Motivated Offenders: The framework deters cybercriminals by increasing the efforts required to access data, thereby reducing the likelihood of exploitation.

For example:

1) Data leakage risks – the framework mandates data sanitization (e.g., clearing, purging, and destruction) based on the device type and data sensitivity.
2) Regulatory gaps – by institutionalizing enforceable policies, the framework responds to participants' observations about the lack of specific e-waste disposal policies.

This alignment between findings and solutions ensures the framework is both practical and grounded in the realities of Tanzanian public institutions.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

### 4.5.2. Device Categorization

Before e-waste devices are disposed of, they are first classified into distinct categories based on their storage types, which also decides the sanitization method, and use cases, as shown in Figure 5.

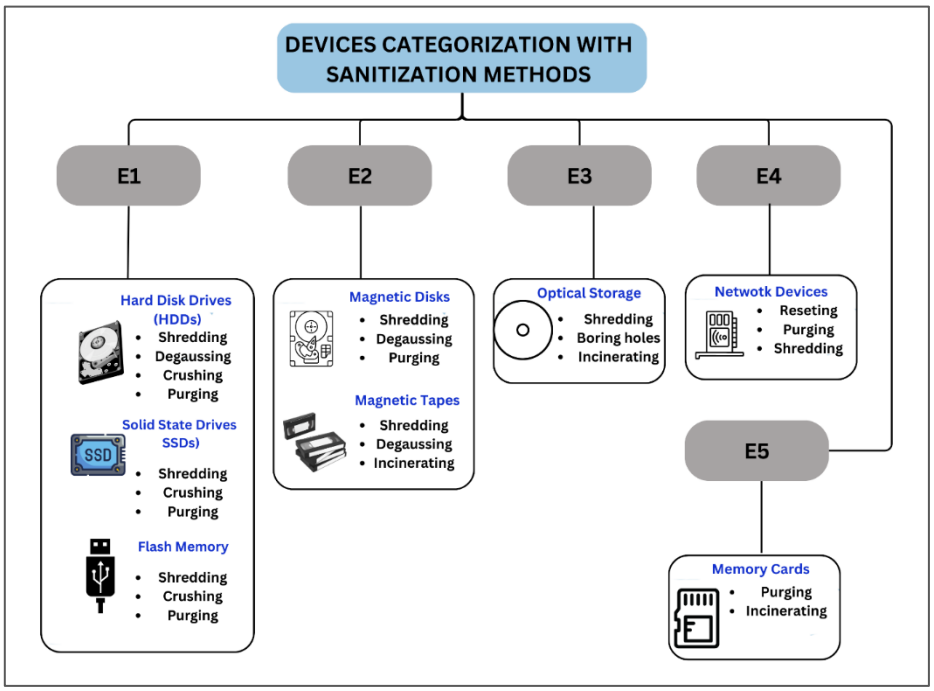


**Figure 5.** Device categorization with their sanitization methods

### 4.5.3. Data sensitivity Assessment

Following classification, the framework evaluates each device's data sensitivity and assigns a score of Low, Moderate, or High depending on the possible consequences of a security breach. This process guarantees that data security is appropriately prioritized during disposal, especially for devices that contain sensitive data. For example, a data breach with a LOW potential impact shows that any breach of confidentiality is likely to have a minimal impact on organizational operations; a MODERATE potential impact indicates that any breach of confidentiality is likely to have a serious negative impact on organizational operations; and a HIGH potential impact indicates that any breach of confidentiality is likely to have a severe or catastrophic adverse effect on organizational operations; see Table 2.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

**Table 2.** Impact level Vs. Adverse effects

| Potential Impact Level | Adverse Effect | Explanation |
|---|---|---|
| Low | Limited | i) Causes a drop in mission performance, allowing only minimal or limited operational tasks.<br>ii) Leads to minor financial losses or resource damage. Result in minor damage to organizational assets<br>iii) Leads to minor individual harm. |
| Moderate | Serious | i) Significantly reduces mission effectiveness or disrupts core functions.<br>ii) Results in notable financial losses or legal ramifications<br>iii) Potentially exposes sensitive information or causes moderate harm to stakeholders. |
| High | Severe | i) Critically impairs or halts the organization's main operations<br>ii) Causes extensive resource damage or infrastructure loss.<br>iii) Leads to major financial setbacks or severe reputational damage.<br>iv) May threaten the safety or well-being of individuals. |

**Note:** Adapted from Standards for Security Categorization of Federal Information and Information Systems (FIPS 199), National Institute of Standards and Technology (NIST).

For low-sensitivity data on functional devices, data clearing/reset is recommended, which involves overwriting data to make recovery difficult but not impossible. After being approved, these devices can either be used again within the company or made accessible to other organizations for usage. A more thorough purging procedure is needed for devices with moderate sensitivity, which successfully eliminates data in a way that hinders all but the most sophisticated recovery attempts. A thorough destroy and recycle strategy is required when devices are thought to be non-functional or contain high-sensitivity data. This includes physically destroying the devices (e.g., shredding or crushing) to remove any chance of data recovery, and then recycling the hardware in an environmentally responsible manner.

All devices go through a validation phase following the initial sanitization stage, during which the procedure's efficacy is confirmed. In order to guarantee adherence to data protection regulations and stop unintentional data breaches, this

is an essential quality control step. Lastly, a reliable audit trail is created by documenting the whole process, which improves accountability and makes regulatory compliance easier. This organized disposal framework not only enhances cybersecurity and promotes regulatory compliance but also lessens the accumulation of e-waste in public institutions through the secure reuse of storage devices.

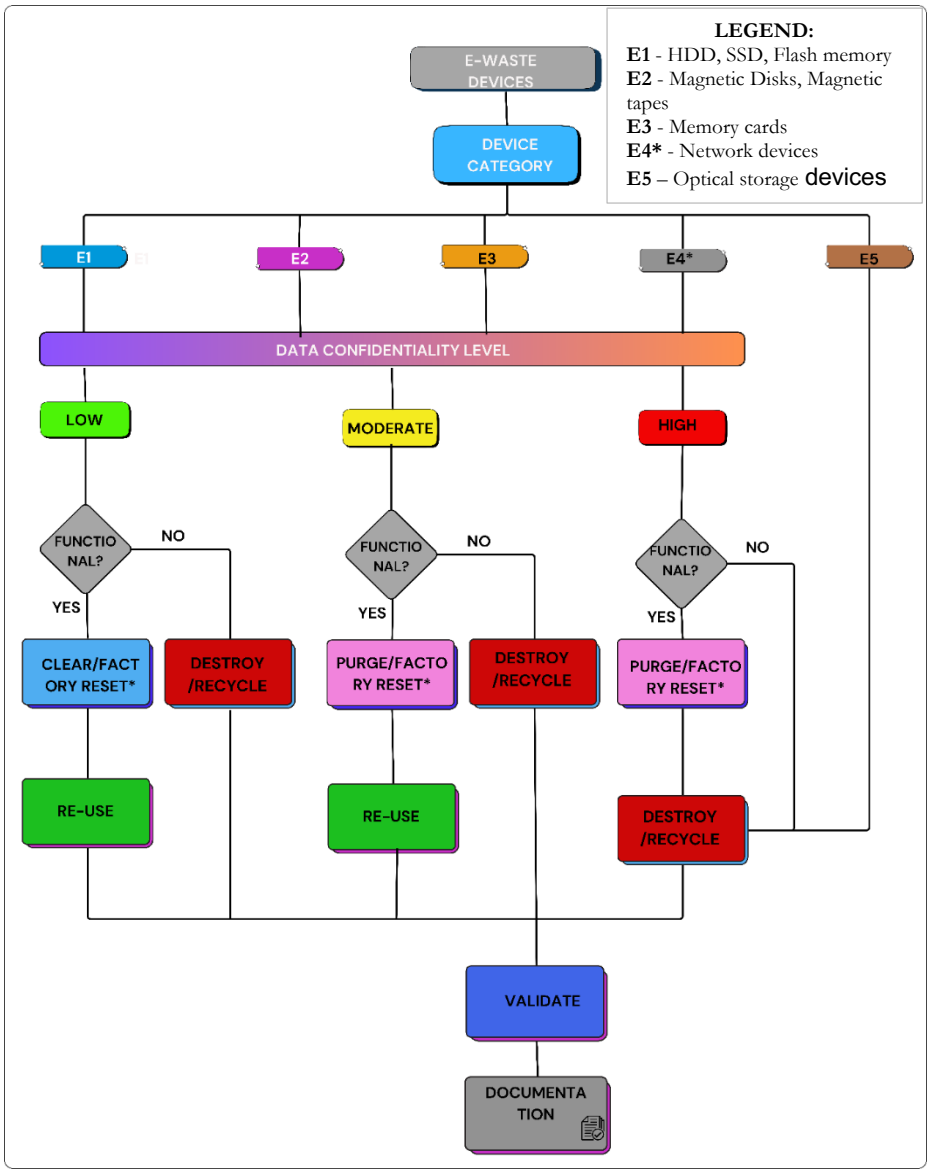


**Figure 6.** The developed disposal framework

### 4.5.4. Study limitation, conclusion, and call for action

This study's insights are constrained by its sample of 11 Tanzanian public institutions, which, while diverse, may not fully capture the range of e-waste disposal challenges across all public sectors. Bureaucratic delays and participant availability further limited data collection scope. However, purposive sampling and data saturation ensured robust findings within the studied context, providing a strong foundation for future research to expand generalizability.

## 5. CONCLUSION

Insecure e-waste disposal in Tanzanian public institutions, exacerbated by inadequate regulations and inconsistent sanitization practices, poses significant cybersecurity risks, including potential data breaches that undermine public trust. These vulnerabilities create a pressing need for a comprehensive solution that safeguards sensitive information and improves e-waste management practices. The proposed Secure E-Waste Disposal Framework directly addresses these challenges by categorizing devices according to data sensitivity and prescribing appropriate sanitization methods ranging from clearing and purging to complete destruction ensuring that sensitive data is adequately protected while also promoting sustainable IT asset management.

For effective change to occur, policymakers and public institutions must take immediate action to adopt secure disposal protocols and integrate the proposed framework into national policies. This will require the establishment of standardized regulations and the implementation of comprehensive staff training on proper data sanitization techniques. These measures are essential not only for mitigating cybersecurity risks but also for aligning with broader circular economy goals. The timely and widespread adoption of these practices is critical to safeguarding institutional data, strengthening e-waste management systems, and fostering greater public confidence in Tanzania's commitment to secure and sustainable technology disposal.

## LIST OF ABBREVIATIONS

| | |
|---|---|
| BYOD | Bring Your Own Device |
| CD | Compaq disk |
| DDP | Device Disposal Practice |
| EEE | Electrical and electronic equipment |
| EOL | End of Life |
| FGD | Focused group discussion |

| | |
|---|---|
| FIPS | Federal Information and Information Systems |
| GCC | Gulf Cooperation Council |
| ICT | Information and Communication Technology |
| IT | Information technology |
| PC | Personal computer |
| PII | Personal Identifying Information |
| RAT | Routine activity theory |
| USB | Universal serial bus |

## REFERENCES

[1] ITU-D, Towards the harmonization of data collection: A baseline study for e-waste in East Africa. 2023.

[2] T. Maes and F. Preston-Whyte, "E-waste it wisely: lessons from Africa," SN Appl. Sci., vol. 4, no. 3, p. 72, 2022, doi: 10.1007/s42452-022-04962-9.

[3] V. Forti, C. P. Balde, R. Kuehr, and G. Bel, "The Global E-waste Monitor 2020: Quantities, flows and the circular economy potential," *2020*.

[4] P. Roychowdhury, J. M. Alghazo, B. Debnath, S. Chatterjee, and O. K. M. Ouda, "Security threat analysis and prevention techniques in electronic waste," in *Waste Management and Resource Efficiency: Proceedings of 6th IconSWM 2016*, Singapore: Springer Singapore, 2018, pp. 853-866.

[5] K. Kusters et al., "The impact of ignorance and bias on information security protection motivation: a case of e-waste handling," *Frontiers in Psychology*, vol. 1, no. 1, pp. 1021–1072, Jun. 2023, doi: 10.3390/land9040128.

[6] N. Ameen Tarhini A., M. H. Shah Madichie N., and J. Paul Choudrie J., "Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce," *Computers in Human Behavior*, vol. 114, 2021, doi: 10.1016/j.chb.2020.106531.

[7] L. Forgor, W. Brown-Acquaye, J. K. Arthur, and S. Owoo, "Security of data on e-waste equipment in Africa: The case of Ghana," in *2019 International Conference on Communications, Signal Processing and Networks (ICCSPN)*, IEEE, 2019, pp. 1–5, doi: 10.1109/ICCSPN46366.2019.9150166.

[8] M. Felson and R. V. Clarke, *Introduction to Crime Science*, SAGE Publications Ltd., 2010.

[9] J. Alghazo, O. K. M. Ouda, and A. El Hassan, "E-waste environmental and information security threat: GCC countries vulnerabilities," *Euro-Mediterranean Journal of Environmental Integration*, vol. 3, no. 1, Nov. 2018, doi: 10.1007/s41207-018-0050-4.

[10] R. K. C. P. Baldé, T. Yamamoto, R. McDonald, E. D'Angelo, S. Althaf, G. Bel, O. Deubzer, E. Fernandez-Cubillo, V. Forti, V. Gray, S. Herat, S. Honda, G. Iattoni, D. S. Khetriwal, V. L. di Cortemiglia, Y. Lobuntsova, I. Nnorom, N. Pralat, and M. Wagner, *The Global E-Waste Monitor 2024 Report*, International Telecommunication Union (ITU) and United Nations Institute for Training and Research (UNITAR), Geneva/Bonn, 2024.

[11] A. Kumar, M. Holuszko, and D. C. R. Espinosa, "E-waste: An overview on generation, collection, legislation and recycling practices," *Resources, Conservation and Recycling*, vol. 122, pp. 32–42, 2017, doi: 10.1016/j.resconrec.2017.01.018.

[12] Magashi, A., and M. Schluep, "E-waste assessment Tanzania," *Cleaner Production Centre of Tanzania & Empa Switzerland*, 2011.

[13] M. N. Bimir, "Revisiting e-waste management practices in selected African countries," *Journal of the Air & Waste Management Association*, vol. 70, no. 7, pp. 659–669, 2020, doi: 10.1080/10962247.2020.1769769.

[14] K. Daum, J. Stoler, and R. Grant, "Toward a More Sustainable Trajectory for E-Waste Policy: A Review of a Decade of E-Waste Research in Accra, Ghana," *International Journal of Environmental Research and Public Health*, vol. 14, no. 2, p. 135, Jan. 2017, doi: 10.3390/ijerph14020135.

[15] N. Kapoor, P. Sulke, and A. Badiye, "E-waste forensics: An overview," *Forensic Science International: Animals and Environment*, vol. 1, p. 100034, 2021, doi: 10.1016/j.fsiae.2021.100034.

[16] P. Szewczyk, K. Sansurooah, and P. A. H. Williams, "An Australian longitudinal study into remnant data recovered from second-hand memory cards," *International Journal of Information Security and Privacy*, vol. 12, no. 4, pp. 82–97, Oct. 2018, doi: 10.4018/IJISP.2018100106.

[17] R. Adams et al., "POPIA Code of Conduct for Research (with corrigendum)," *South African Journal of Science*, vol. 117, no. 5/6, May 2021, doi: 10.17159/sajs.2021/10933.

[18] R. Ichikowitz and T. Hattingh, "Consumer e-waste recycling in South Africa," *South African Journal of Industrial Engineering*, vol. 31, no. 3, Nov. 2020, doi: 10.7166/31-3-2416.

[19] L. Godfrey and S. Oelofse, "Historical review of waste management and recycling in South Africa," *Resources*, vol. 6, no. 4, p. 57, Oct. 2017, doi: 10.3390/resources6040057.

[20] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in *2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE)*, IEEE, Apr. 2014, pp. 189–192, doi: 10.1109/ISCAIE.2014.7010235.

[21] M. Alqahtani and R. Braun, "Reviewing influence of UTAUT2 factors on cyber security compliance: A literature review," *Journal of Information Assurance and Cybersecurity*, vol. 2021, pp. 1–15, May 2021, doi: 10.5171/2021.666987.

[22] T. Escobar-Rodríguez and E. Carvajal-Trujillo, "Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model," *Tourism Management*, vol. 43, pp. 70–88, Aug. 2014, doi: 10.1016/j.tourman.2014.01.017.

[23] M. T. Whitty, "419 – It's just a game: Pathways to cyber-fraud criminality emanating from West Africa," 2018, doi: 10.5281/ZENODO.1467848.

[24] Y. S. Lincoln, S. A. Lynham, and E. G. Guba, *Paradigmatic Controversies, Contradictions, and Emerging Confluences Revisited*, N. K. Denzin & Y. S. Lincoln, Eds., 4th ed., Sage, 2011.

[25] C. Andrade, "The inconvenient truth about convenience and purposive samples," *Indian Journal of Psychological Medicine*, vol. 43, no. 1, pp. 86–88, Jan. 2021, doi: 10.1177/0253717620977000.

[26] S. K. Sharma, S. K. Mudgal, R. Gaur, J. Chaturvedi, S. Rulaniya, and P. Sharma, "Navigating sample size estimation for qualitative research," *Journal of Medical Evidence*, vol. 5, no. 2, pp. 133–139, Apr. 2024, doi: 10.4103/JME.JME_59_24.

[27] D. Byrne, "A worked example of Braun and Clarke's approach to reflexive thematic analysis," *Quality & Quantity*, vol. 56, no. 3, pp. 1391–1412, Jun. 2022, doi: 10.1007/s11135-021-01182-y.

[28] T. Maes and F. Preston-Whyte, "E-waste it wisely: Lessons from Africa," *SN Applied Sciences*, vol. 4, no. 3, Mar. 2022, doi: 10.1007/s42452-022-04962-9.

[29] J. Alghazo and O. K. Ouda, "Electronic waste management and security in GCC countries: A growing challenge," in *Proceedings of the ICIEM International Conference*, Sousse, Tunisia, Oct. 2016, pp. 27-30.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

**Appendix A:** Interview and Focused Group Discussion guide

**A: Open-Ended Interview guiding Questions for E-Waste Disposal and Cybersecurity**

**Based on the specific objectives, here are some open-ended questions for respondent's interviews:**

**Specific Objective 1: (**To investigate e-waste disposal practices in public institutions)

1) Can you describe the current e-waste management procedures used by your institution?
2) What specific concerns do you have regarding potential vulnerabilities created by these procedures?
3) Have you encountered any instances where insecure e-waste disposal led to a cybersecurity breach? If so, could you share details without compromising security?
4) In your opinion, what are the main gaps in current knowledge or practices that contribute to vulnerabilities in cyber security related to e-waste?

**B: Guiding Questions for Focused group discussion**

Focused Group Discussion questions on secure e-waste disposal practices for public institutions:
Introduction: Introduced the topic

**Opening Questions**

1) In your experience, what are the main challenges public institutions face regarding secure e-waste disposal?
2) What are the biggest concerns related to cybersecurity threats from the current disposal practices of electronic devices?
3) Can you share any specific examples (if any) of data breaches or security incidents caused by insecure e-waste disposal in public institutions?
4) What existing policies or regulations are in place to govern e-waste disposal in your institutions? Are they effective?