OFFICE OF INDEPENDENT INTERNAL AUDIT

DeKalb County
GEORGIA

December 2025

DeKalb County Government
County-wide

AUDIT OF MOBILE DEVICE INVENTORY AND MANAGEMENT

FINAL REPORT

Lavois Campbell, CIA, CISA, CFE, CGA
Chief Audit Executive

Audit Report No. IA-2025-0275-IT

Legal Redaction Disclaimer

Pursuant to **O.C.G.A. § 50-18-72(25)(A)** of the Georgia Open Records Act, certain sections of this report have been redacted. These redactions protect sensitive information, the disclosure of which could reasonably be expected to compromise security against sabotage, criminal, or terroristic acts. The withheld information may include security procedures, infrastructure details, or system vulnerabilities that, if publicly disclosed, could jeopardize public safety or operational integrity.

DeKalb County GEORGIA

Lavois Campbell
Chief Audit Executive

AUDIT OF MOBILE DEVICE INVENTORY AND MANAGEMENT
REPORT NO. IA-2025-0275-IT

FINAL REPORT

HIGHLIGHT SUMMARY

Why We Performed the Audit

We audited the County's mobile device inventory and management to assess governance and controls across the device lifecycle—assignment, use, return, and decommissioning—and their alignment with operational and security needs. We conducted this audit as a strategic initiative to bolster security, identify devices that are underutilized, verify that all devices adhere to organizational policies and procedures, facilitate better management of the device lifecycle from procurement to retirement and ensuring that employees have access to functioning and appropriate devices. Weaknesses in these areas heighten risks of data breaches, asset loss, noncompliance, and inefficiency. Our findings and recommendations aim to strengthen lifecycle controls, improve accountability, enhance security, and optimize resources.

How We Performed the Audit

The audit focused on the Department of Innovation and Technology's (DoIT) processes for the management of mobile devices, including assignment, utilization, return, and decommissioning. Our methodology included, but was not limited to, the following:

- Researched related best practices.
- Reviewing policies, best practices, and sample, inventory, assignment, compliance, and disposal records.
- Conducting process walkthroughs and interviews with DoIT personnel.
- Analyzing documentation for compliance and risk management

Background

DoIT manages the full lifecycle of County-issued devices—laptops, phones, tablets/iPads, and hotspots. Requests (new hires, replacements, swap-outs) flow through the ticketing system. Assets are tracked in the Verizon Business Portal (mobile lines), Absolute (laptops), and M crosoft Intune (security/configuration). Surplus equipment is kept in secured, restricted areas. This audit assesses the accuracy, completeness, and cost-effectiveness of these processes across procurement, assignment, use, return, and decommissioning.

What We Found

The audit found that DoIT has established processes and implemented tools to support the management of mobile devices. These include the use of Verizon's portal for mobile phones and hotspots, Absolute for laptops, and Microsoft Intune for device management and security enforcement. Device assignments are managed through the ticketing system, and departments conduct monthly reviews of cell phone bills to monitor usage. Devices that remain inactive for 60 days are flagged for deactivation.

Additionally, the governing policies for mobile device management are outdated and incomplete. The Utilization of Technologies Policy remains in draft form and, together with the Information Security Policy, does not comprehensively address all device types in use or establish clear requirements for employees to return County-issued devices or formally acknowledge receipt and understanding of the policies.

Audit Observation

1. **Inadequate Mobile Devices Policies increase Data Security and Asset Loss Risk**
2. **Absence of Documentation Undermines Mobile Devices Lifecycle Controls**
3. **Inadequate Disposal Records Prevent Verification of Secure Data Destruction**
4. **Challenges in Data Protection** [redacted]

What We Recommend

We recommend that the DoIT management address the control process deficiencies identified in this report.

How Management Responded

Management accepted all audit findings and has action plans to address them by March 2026.

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

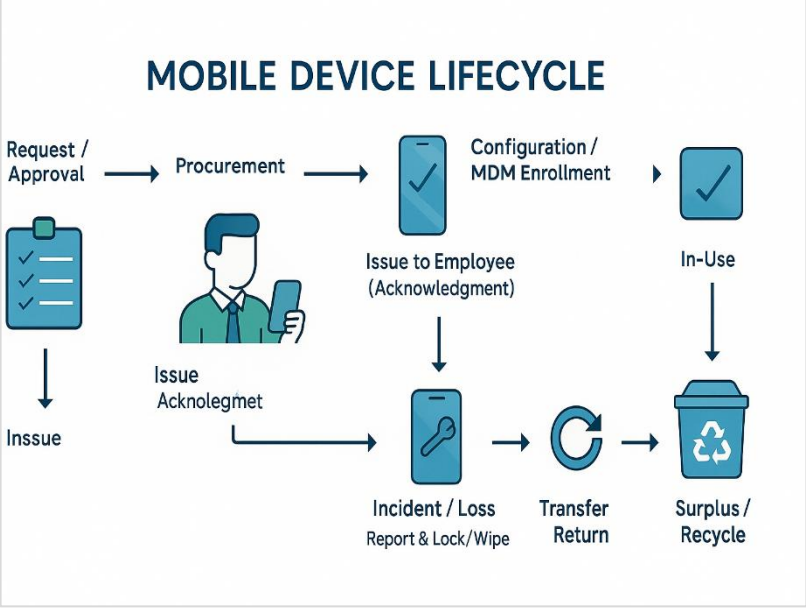
Mobile Device Inventory and Management (MDIM) refers to the coordinated processes, tools, and controls used to procure, track, secure, and manage mobile devices throughout their lifecycle from acquisition and deployment to reassignment, retirement, and disposal. DoIT Management provided the purchase history of IT devices for the period spanning from March 2023 to April 2025. Our analysis of this data indicated that a total of 2706 laptops were ordered, amounting to 4.56 million USD.

Effective MDIM ensures that devices are accounted for, protected against unauthorized access, and utilized efficiently to support organizational operations.

Employees across the County utilize mobile devices to perform a variety of work-related functions, including accessing County systems, communicating with colleagues, and supporting service delivery to residents. The Department of Innovation and Technology (DoIT) is responsible for overseeing the deployment, tracking, and lifecycle management of all County-issued mobile devices. Common devices include laptops, cell phones, iPads, and tablets, as well as connectivity tools such as mobile wi-fi (MiFi) cards and portable hotspots.

The County procures and manages wireless services through two government-wide contracts, one with the Georgia Technology Authority (GTA) and another with the Federal General Services Administration (GSA). Both contracts identify Verizon as the County's primary wireless service provider for cell phones, tablets, iPads, and hotspots. Laptop devices are acquired through a piggyback agreement with Dell Marketing, L.P., under Georgia Statewide Contract.

The County's centralized service ticketing system is used for requesting resources for new hires, replacements, and device swap-outs. Information such as phone numbers, **International Mobile Equipment Identity** (IMEI), and model numbers is available in the Verizon Business Portal, while laptops are tracked in [redacted] using device serial numbers as asset identifiers. This integration **is intended to support** consistent recordkeeping and **enhance**



accountability for device assignment and reassignment.

The County **has deployed** [redacted] for Mobile Device Management (MDM), integrated with Active Directory and Azure, **to manage** configuration and security policies and provide remote administration capabilities. **According to DoIT procedures,** devices with no recorded usage for 60 days are flagged for potential deactivation during monthly departmental billing reviews and are **subject to** further evaluation by DoIT through a 60 day zero-usage review. These reviews are intended to reduce costs and prevent unnecessary access to County systems.

Surplus equipment is stored in secure, badge-restricted facilities. **According to management,** during the employee exit interview with Human Resources, the employee is required to return all County assets before the next paycheck. Lifecycle planning and inventory oversight **are designed to be** further supported by dashboards generated from [redacted] and Verizon, which provide DoIT with visibility into device activity, compliance, and utilization. **DoIT's process for** decommissioned laptops **states that** hard drive destruction is performed by third-party vendors; County staff are present to visually confirm destruction and retain documentation such as Certificates of Destruction for accountability and audit purposes.

As reliance on mobile devices increases across County operations, strong policies, consistent lifecycle management practices, and robust security controls have become essential to protect sensitive information, reduce risks, and safeguard public assets. This audit was conducted to assess the accuracy, completeness, and effectiveness of the County's mobile device inventory and management processes, including assignment, utilization, return, and decommissioning practices, and to evaluate whether governance structures, tools, and procedures are in place to adequately protect sensitive information.

Why this Audit Was Performed

The effective management of the County's mobile device inventory is critical to maintaining secure, and efficient operations. Mobile devices including laptops, tablets, smartphones, and hotspots are essential tools that enable employees to access County systems, communicate, and deliver public services. Given that these devices store or transmit sensitive information and are frequently used outside the County's secure network, robust management and oversight are paramount to protecting County data and assets.

Weaknesses in mobile device management, such as incomplete inventory records, inadequate tracking of device assignment and return, insufficient monitoring of inactive devices, or unverified secure decommissioning of retired assets, create significant risks. These risks include data breaches, unauthorized access, loss or misuse of County property, non-compliance with regulatory requirements, operational disruptions, and increased costs. Industry standards, including **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Rev. 2** and **NIST SP 800-53 Rev. 5**, emphasize the

necessity of clear policies, accurate inventory, strong security configurations, and documented processes to mitigate these exposures.

This audit provides an independent assessment of the County's mobile device lifecycle, from assignment and active use to return and disposal. It aims to confirm that these activities are well-managed, cost-effective, and supported by effective internal controls. By identifying areas for improvement, this audit helps strengthen oversight, enhance data protection, ensure responsible resource management, and ultimately build public trust in the County's ability to safeguard its information and assets.

Our Scope, Objectives, and Methodology

This audit's primary objective was to assess the accuracy, completeness, and cost-effectiveness of the County's mobile device inventory and management processes. This included evaluating the adequacy of related governance, security controls, and compliance with relevant policies and industry standards, specifically NIST SP 800-124 and NIST SP 800-53. Using NIST SP 800-124 and SP 800-53 as criteria, we reviewed inventory tracking, security configuration, and lifecycle management.

The audit focused on the following key areas to ensure mobile devices are properly tracked, securely configured, and managed from acquisition through disposal:

- **Governance structures:** Including policies, roles, and responsibilities.
- **Procurement and Assignment:** Processes for acquiring and distributing mobile devices.
- **Inventory Tracking:** Methods for managing and reconciling device inventory.
- **Return and Offboarding:** Procedures for separated employees.
- **Surplus and Disposal:** Practices, including documentation such as Certificates of Destruction and Transfer of Responsibility forms.
- **Mobile Device Management (MDM) Tools:** Implementation and use of [redacted] and [redacted].
- **Security Controls:** Measures applied to protect County-issued devices and sensitive information.

The scope of this engagement included all County-issued laptops, tablets (including iPads), smartphones, and mobile hotspots for the period of January 1, 2023, through June 30, 2025.

Audit procedures included walkthroughs and interviews with staff from the Department of Innovation and Technology (DoIT). We also conducted comprehensive reviews of documentation and reports from the County's ticketing system, the Verizon Business Portal, [redacted], and [redacted]. Furthermore, selected records related to procurement, assignment, inventory reconciliation, and disposal were tested to evaluate the design and operating effectiveness of controls.

Sampling Methodology, Size, and Population

The audit team used a judgmental sampling methodology to assess the accuracy, completeness, and effectiveness of the County's mobile device inventory and management controls. This approach was selected based on auditor judgment to focus testing on areas of higher risk and operational significance, where control failures would have the greatest impact. Judgmental sampling was appropriate for this engagement because the objective was to evaluate control design and operating effectiveness, rather than to draw statistically projected conclusions for the entire population.

The Department of Innovation and Technology (DoIT) submitted 23 records representing all devices disposed of during the audit period. The audit team performed a 100-percent review of these records to confirm that disposal documentation was properly maintained, reconciled, and aligned with the County's data sanitization and accountability requirements.

AUDIT RESULTS

The Department of Innovation and Technology (DoIT) has established processes and uses key tools to manage mobile devices, including the Verizon Business Portal, [redacted], and [redacted]. While procedures exist for device procurement, assignment, and usage reviews, the audit identified **significant gaps in governance, lifecycle controls, and data protection.**

We found that foundational policies are outdated, incomplete, and not formally approved, leading to inconsistent practices. Critical documentation for device assignment, return, and disposal is not consistently maintained, which prevents a complete audit trail and weakens accountability. Most critically, these control failures leave County data exposed. **A significant number of devices are [redacted], and thousands of devices are "dark" or unmonitored**, creating a high risk of data breach and asset loss.

This report presents the detailed findings and corresponding recommendations to formalize governance, improve recordkeeping, and urgently address the security and lifecycle management of the County's mobile device program.

Finding 1 – Inadequate Mobile Device Policies Increase Data Security and Asset Loss Risks

Through review of the Information Security Policy (ISP) and Utilization of Technologies Policy, it was determined that DeKalb County's mobile device inventory and management policies and procedures require enhancement. We noted the following:

1. The Utilization of Technologies Policy did not fully reflect the range of mobile devices actively deployed across the County. The definition did not include iPads, tablets, and portable hotspot devices.

2. The Utilization of Technologies Policy remains in draft form and has not been formally approved. Although the draft version provides some guidance, it does not carry the authority of an adopted County policy.

3. There is no requirement within the policies for employees to return County-issued devices upon separation or reassignment, and the Utilization of Technologies Policy does not require employees to acknowledge that they have received and understood the policy.

4. The Information Security Policy and the Utilization of Technologies Policy available on the intranet are outdated. The Information Security Policy shows an effective date of July 1, 2016 but no sign off date, while the Utilization of Technologies Policy is dated April 2017.

NIST SP 800-124 Revision 2 section 5.4.2.(Device Usage): An organization should develop security and privacy policies for mobile device (and app) usage.

NIST SP 800-124 Rev 2 Section 4.3.11. (Mobile Device Security Policies) states that the development of security policies is vital to establishing a prominent security posture through well-defined procedures and governance.

International Organization for Standardization (ISO)27001:2022 Annex A Control 5.11, emphasizing the secure return of organizational assets when roles or contracts end, to prevent data breaches and ensure compliance with information security policies.

These policy deficiencies prevent the County from enforcing consistent governance over mobile technology and leave it vulnerable to significant risks. The exclusion of commonly issued devices, the omission of requirements for device returns, and the absence of employee acknowledgment requirements increase the County's exposure to inconsistent practices, data security vulnerabilities, and challenges in holding employees accountable for misuse or noncompliance.

Recommendations

We recommend that DoIT strengthen mobile device Inventory and management governance by updating and formalizing the Information Security Policy (ISP) and the Utilization of Technologies Policy (UTP). Management should:

- Update the Utilization of Technology Policy to include all County-issued mobile

devices in use (e.g., iPads, tablets, portable hotspots) and define controls applicable to each device type.

- Finalize and obtain formal approval of the Utilization of Technologies Policy so it can be enforced consistently across the County.
- Incorporate requirements for employees to (a) acknowledge receipt and understanding of the Utilization of Technologies Policy, and (b) return all County-issued devices upon separation, transfer, or reassignment, and integrate this into the offboarding process.
- Update the ISP to replace the outdated policy on the intranet and ensure it reflects current practices. The Utilization of Technologies Policy should be finalized and published on the intranet, so employees have access.

Management Response (Department of Innovation & Technology Management):

Management Agreement	***Description of Management's Action Plan to Address Finding***	***Estimated Timeline to Implement Action Plan***
☒ Agree **☐ Disagree**	**The ISP is currently being updated. The Acceptable Use Policy, or UTP is already in CV360 as an onboarding task.**	**3/31/2026**
Additional Comments (if Any)- Max 150 words.:		

Finding 2 – Absence of Documentation Undermines Mobile Device Lifecycle Controls

During the planning phase of the Mobile Device Management audit, the audit team requested supporting documentation to evaluate oversight and compliance with established processes. The documentation requested was not readily available for review. **Management indicated that compiling the necessary data for procurement, assignment, inventory tracking, return, offboarding, and asset disposal activities would require an estimated 3-6 months**, confirming the absence of readily accessible and reconciled records. **Specifically:**

- **Overall Inventory:** A complete, year-end inventory report reconciling all County-issued laptops, tablets, mobile hotspots, and smartphones.
- **Deployment:** Acknowledgment forms for devices issued to employees are not consistently maintained or centrally retained.
- **In-Life Management:**
    - A list of approved software inventory (blacklist/whitelist), including authorized and prohibited software for mobile devices.
    - Reports demonstrating the monitoring and enforcement of Mobile Device Management (MDM) policies.
    - Evidence of review and sign-off by Heads of Department for monthly cell phone usage bills.

- **End-of-Life Management:**
    - Acknowledgment forms for devices returned by separated or transferred employees.
    - A reconciled and complete list of surplus devices.
    - Records confirming that mobile devices were securely reimaged or wiped prior to redeployment or destruction.

NIST Special Publication 800-53, control related to CM-8 (System Component Inventory): The organization develops and documents an inventory of system components that: (a) accurately reflects the current system; (b) includes all components within the authorization boundary of the system; (c) is at the level of granularity deemed necessary for tracking and reporting; and (d) is reviewed and updated regularly.

The **systemic absence of this critical documentation, coupled with management's estimate that compiling the necessary data would require an estimated 3-6 months,** severely reduces accountability, limits management's ability to monitor, and weakens assurance over the entire device lifecycle. This profound failure to maintain readily available records directly increases the County's exposure to:

- **Financial Loss:** From the theft or loss of unmonitored assets that are never reported missing.
- **Data Breaches:** From lost, stolen, or improperly surplus devices that still contain sensitive County data.

- **Non-optimal Use of Funds:** From continuing to pay for device service plans that are no longer in use or needed.

Recommendations

We recommend that DoIT management strengthen lifecycle controls and accountability by taking the following actions:

1. **Establish Foundational Inventory:** Prepare an annual inventory report reconciling all County-issued devices and have it reviewed by a Governance Risk Compliance (GRC) officer.
2. **Control Deployment & Return:** Establish a standardized acknowledgment form for all devices issued and returned, and ensure these records are centrally maintained and readily retrievable for audit and oversight.
3. **Enforce In-Life Controls:** Develop and maintain an approved application list (blacklist/whitelist), enforced through the MDM tool.
4. **Monitor Compliance:** Generate periodic compliance reports and retain evidence of review by the Security/GRC team.
5. **Monitor Usage:** Recommend that each Cost Center Owner, or designee, conduct a documented review of monthly mobile usage. The reviews should be signed and retained by DoIT.
6. **Secure Re-deployment:** Develop procedures for recording device resets, hard drive replacements, and reimaging activities to provide assurance that devices are securely wiped prior to reassignment.
7. **Secure Disposal:** Maintain a reconciled surplus/unusable inventory and align it with vendor certificates of destruction if the asset is to be destroyed.
8. **Implement a Strategic Solution:** To ensure these processes are efficient, consistent, and sustainable, develop or acquire a formal asset management system to improve tracking, accountability, and the immediate availability of all relevant documentation for management review and regulatory compliance.

Management Response (Department of Innovation & Technology Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Agree ☐ Disagree	Currently collecting inventory of devices in [redacted].	3/31/2026 – Devices in [redacted]
Additional Comments (if Any)- Max 150 words.: Need to work with HR on tracking the issued and returned devices in CV360. [redacted]. Agree to wipe all cell phones and iPads prior to re-issue.		

Finding 3 - Inadequate Disposal Records Prevent Verification of Secure Data Destruction

DoIT submitted a total of 23 records on disposal of assets for the audit period. We conducted a 100 percent review of the documents, and the breakdown is as follows: 7 Certificates of Destruction (CODs), 6 Transfer of Responsibility (TOR) forms, 7 Recycling Detail Certificates (RDCs), 1 Data Destruction Certificate (DDC), 1 Certificate of Recycling (RC), and 1 Missiletag (**sheet for tracking details of devices**) Log.

- **Eighteen of the 23 records lacked a complete count of hard drives and did not include a detailed inventory** of laptops, tablets, iPads, iPhones, and portable hotspots provided to the vendor for destruction.
- **Some of the reviewed records also lacked sufficient details such as asset tags**, serial numbers, or other identifiers to reconcile disposed devices with County-owned assets across all document types (CODs, TORs, RDCs, DDC, RC, and Missiletag Log).
- **In addition, 14 of the 23 records were missing County certification signatures confirming verification of the destroyed devices.**
- The Audit team could not reconcile the data provided because **comprehensive inventory of the devices was not readily available.**

NIST SP 800-88r2, Guidelines for Media Sanitization (September 2025), Section 4.6 Documentation, recommends that the certificate should record at least the following details:

- Manufacturer, Model, Serial number
- Organizationally assigned media or property number (if applicable), Media type (i.e., hard copy or ISM), Media source (e.g., user, computer)
- Pre-sanitization confidentiality categorization (optional), Sanitization method (i.e., clear, purge, destroy)
- Sanitization technique (e.g., degauss, overwrite, block erase), Tool used, including version
- Verification method - Information of individuals performing verification and validation: Name of person, Position/title of person, Date, Location, Contact information (e.g., phone number), Signature.

The absence of reconciled, comprehensive records increases the risk of:

- Loss or misappropriation of County-owned assets.
- Inability to confirm proper destruction of devices containing sensitive data.
- Non-compliance with industry standards and statutory requirements for data sanitization.

In addition, missing signatures can lead to disputes in future.

Recommendations

We recommend that DoIT should:

- Update the Transfer of Responsibility forms to include a comprehensive inventory of all items provided to the vendor for destruction, specifically identifying laptops, tablets, iPads, iPhones, portable hotspots, and the count of hard drives.
- Require signed documentation at the point of handoff, with acknowledgment from both DoIT and the vendor, to confirm reconciliation of devices to County asset records.
- Retain all disposal records in a centralized repository (e.g., CV360) to ensure accountability, auditability, and compliance.
- Incorporate validation process in the disposal of any media or system components, especially that which contains PII or sensitive information.
- Develop and Implement Certificate of Sanitization Form similar to NIST 800-88R2 Appendix C.

Management Response (Department of Innovation & Technology Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	**For laptops, working with the vendor to develop the necessary forms for recycling equipment.**	**3/31/2026**
Additional Comments (if Any)- Max 150 words.: For mobile phones, we will work on a similar process for return of devices.		

Finding 4. Challenges in Data Protection [redacted]

During our review, it was observed that data protection measures have not been consistently applied across the County's mobile devices in alignment with the sensitivity of data at rest or in transit. The devices covered in this review include:

- Windows laptops (180 devices)
- Apple iOS/iPadOS devices (917 devices)
- Android devices (514 devices)

Currently, DoIT has deployed [redacted] for endpoint security and data risk management. In our review of the [redacted] dashboard, we noted the following:

1. About **122 devices are unprotected** because they are unlicensed.
2. A total of **2685 unused devices over the last 30 days.** DoIT management explained that the devices could be surplus.
3. **About 2700 dark devices (devices not functioning, turned off or used for malicious activities)** recorded over the last 90 days
4. [redacted] **percent of devices**

The audit team also reviewed reports generated from the [redacted] **dashboard**, which is used to enforce encryption standards and provide oversight.

In our analysis, we noted the following:

- The [redacted] which is considered safe and effective; however, for highly sensitive data or environments, larger key sizes should be considered if feasible.
- A [redacted] revealed that several [redacted].
- Additionally, from [redacted], **mobile devices such as iPhones** were found to [redacted].

NIST Special Publication 800-53, control related to SC-13 Cryptographic Protection: "Employ cryptographic protection for information at rest, information in transit, and information during use where cryptographic protection is required.
SC-28 Protection of Information at Rest: "Protect the confidentiality and integrity of information at rest.

The absence of [redacted] may have resulted in the belief that the current data security measures [redacted].

The failure to [redacted] fleet and ensure compliance on mobile devices leaves sensitive County data unprotected. This creates a

high, immediate risk of a data breach from a lost or stolen device, which could lead to significant financial, legal, and reputational damage. Furthermore, this is a direct violation of NIST security standards.

Recommendations:

We recommend that DoIT strengthen data protection and asset visibility by taking the following actions:

To Address Unmonitored & At-Risk Devices:

- **1. Investigate "Dark" and Unlicensed Devices:** Immediately investigate all devices reported as "dark" (not seen in 90 days) or "unlicensed." Remediate the devices, secure them, or formally document them as lost/retired to eliminate unmonitored security risks.
- **2. Manage "Unused" Assets:** Develop a process to review “unused” devices for 30 days. This process should aim to recover, redeploy, or retire these assets to reduce license costs and shrink the potential attack surface.

To Addres

- [redacted] Ensure 100% of County-issued mobile devices (laptops, tablets, and phones) are enrolled in [redacted] to enforce consistent security policies.
- **4.** [redacted]**:** Expand [redacted] coverage to all Windows laptops and [redacted] on all iOS/Android devices.
- **5. Monitor and Remediate:** Establish a recurring process to centrally monitor [redacted]ne. All non-compliant devices, including those with [redacted], must be investigated and remediated promptly.

Management Response (Department of Innovation & Technology Management):

Management Agreement	*Description of Management’s Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ Agree ☐ Disagree	**We currently have a process in place with [redacted] non-usage for 60 days.**	**3/31/2026**
Additional Comments (if Any)- Max 150 words.: Already working to get all county-issued mobile devices enrolled in InTune by 3/31/2026. InTune can manage expanding the BitLocker coverage.		

APPENDICES

APPENDIX I – PURPOSE, SCOPE, AND METHODOLOGY

Purpose

The purpose of this audit was to evaluate the accuracy, completeness, and management of the County's mobile device inventory, with particular emphasis on the role of the Mobile Device Management (MDM) system in tracking, securing, and ensuring compliance for all devices accessing County resources.

The audit also aimed to determine whether governance structures, lifecycle processes, and security controls for mobile devices are appropriately designed and operating effectively to safeguard sensitive data, support accountability, and promote cost-effective use of public resources.

Scope and Methodology:

The audit scope covered the period from January 1, 2023, to June 30, 2025, and included laptops, tablets (including iPads), smartphones, and mobile hotspots.

Our methodology included, but was not limited to, the following:

- Researched related best practices.
- Reviewing policies, best practices, and sample, inventory, assignment, compliance, and disposal records.
- Conducting process walkthroughs and interviews with DoIT personnel.
- Analyzing documentation for compliance and risk management

Sampling Methodology, Size, and Population

The audit team used a judgmental sampling methodology to assess the accuracy, completeness, and effectiveness of the County's mobile device inventory and management controls. This approach was selected based on auditor judgment to focus testing on areas of higher risk and operational significance, where control failures would have the greatest impact. Judgmental sampling was appropriate for this engagement because the objective was to evaluate control design and operating effectiveness, rather than to draw statistically projected conclusions for the entire population.

The Department of Innovation and Technology (DoIT) submitted 23 records representing all devices disposed of during the audit period. The audit team performed a 100-percent review of these records to confirm that disposal documentation was properly maintained, reconciled, and aligned with the County's data sanitization and accountability requirements.

APPENDIX II – MANAGEMENT RESPONSE

DEKALB COUNTY DoIT
DEPARTMENT OF INNOVATION & TECHNOLOGY

Interim Chief Information Officer
Scott Shelton

Chief Executive Officer
Lorraine Cochran-Johnson

Board of Commissioners
District 1
Robert Patrick

District 2
Michell Long Spears

District 3
Nicole Massiah

District 4
Chakira Johnson

District 5
Mereda Davis Johnson

District 6
Edward "Ted" Terry

District 7
LaDena Bolton

12/4/2025

Lavois Campbell
Chief Audit Executive
Office of Independent Internal Audit
1300 Commerce Drive, Suite 300
Decatur, Georgia 30030

RE: **Management Response to "Audit of Mobile Device Inventory and Management - Audit Report No. IA-2024-0275-IT**

Dear Mr. Campbell:

In accordance with DeKalb County, Georgia – Code of Ordinances / Organizational Act Section10A-Independent Internal Audit, this is our response to the audit named above provided in this document. As required by the ordinance, our response includes 1) a statement regarding our agreement or disagreement along with reasons for any disagreement, 2) our plans for implementing solutions to issues identified, and 3) the timetable to complete such plans.

If you have any questions about this response, please contact me.

Sincerely,

Scott Shelton

Shelton, Scott
Interim Chief Information Officer,
Department of Innovation & Technology

3630 Camp Circle | Decatur, GA 30032 | phone: 404-371-2847 |
www.dekalbcountyga.gov

APPENDIX III – Definitions and Abbreviations

Acronyms and Abbreviation

DoIT: Department of Innovation and Technology.

MDM: Mobile Device Management

COD: Certificates of Destruction

TOR: Transfer of Responsibility

RDC: Recycling Detail Certificates

DDC: Data Destruction Certificate

RC: Certificate of Recycling

NIST: National Institute of Standards and Technology

MDIM: Mobile Device Inventory and Management

GTA: Georgia Technology Authority

GSA: Federal General Services Administration

IMEI: International Mobile Equipment Identity

Key Definitions

Mobile Device Inventory and Management (MDIM): MDIM refers to the processes, tools, and controls used to account for, monitor, and safeguard mobile devices including laptops, tablets, smartphones, and portable hotspots throughout their lifecycle, from procurement and deployment to reassignment, retirement, and disposal.

From an IT audit perspective, effective MDIM is critical to ensuring that all devices are accurately inventoried, securely configured, and compliant with established policies and standards such as NIST SP 800-124, NIST SP 800-53, and NIST SP 800-88r2. Proper MDIM practices help prevent unauthorized access, data loss, and misuse of public assets, while supporting accountability and efficient use of technology resources.

DISTRIBUTION

Action Distribution:

Shelton Scott, Interim CIO, Department of Innovation & Technology
Alexandro Betancourt Deputy Director Innovation, DoIT

Statutory Distribution:

Lorraine Cochran-Johnson, Chief Executive Officer

Robert Patrick, Board of Commissioners District 1

Michelle Long Spears, Board of Commissioners District 2

Nicole Massiah, Board of Commissioners District 3

Chakira Johnson, Board of Commissioners District 4

Mereda Davis Johnson, Board of Commissioners District 5

Ted Terry, Board of Commissioners Super District 6

LaDena Bolton, Board of Commissioners Super District 7

Tanja Christine Boyd-Witherspoon, Chairperson, Audit Oversight Committee

Adrienne T. McMillion, Vice -Chairperson, Audit Oversight Committee

Lisa Earls, Audit Oversight Committee

Michael Lopata, Audit Oversight Committee

Petrina Bloodworth, Audit Oversight Committee

Information Distribution:

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

Dr. G. Leah Davis, CEO's Chief of Staff

Barbara H. Sanders, BOC Chief of Staff

William “Bill” Linkous, County Attorney

PROJECT TEAM

This report was submitted by:

Not availble for signiture — 12.08.2025

Tolu Ologbenla, MBA, CISA, CISM, CRISC, CCAK, PMP, CSM — Date
IT Internal Auditor, Senior
Office of Independent Internal Audit

This report was reviewed by:

Maxwell Addico — 12.08.2025

Maxwell Addico, MBA, CISA, ISO/IEC 27001 LA — Date
IT Audit Manager
Office of Independent Internal Audit

The report was approved by:

Lavois Campbell — 12.08.2025

Lavois Campbell, CIA, CISA, CFE, CGA — Date
Chief Audit Executive
Office of Independent Internal Audit

STATEMENT OF ACCORDANCE

Statement of Accordance

The mission of DeKalb County is to make the priorities of the citizens of DeKalb County; the priorities of County government - by achieving a safer DeKalb, building stronger neighborhoods, creating a fiscally accountable and more efficient county government, and uniting the citizens of DeKalb County.

The mission of the Office of Independent Internal Audit is to provide independent, objective, insightful, nonpartisan assessment of the stewardship or performance of policies, programs, and operations in promoting efficiency, effectiveness, and integrity in DeKalb County.

This performance audit was prepared pursuant to DeKalb County, Georgia – Code Ordinances/Organizational Act Section10A- Independent Internal Audit. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report is intended for the use of the agency to which it was disseminated and may contain information that is exempt from disclosure under applicable law. Do not release without prior coordination with the Office of Independent Internal Audit.

Please address inquiries regarding this report to the Office of Independent Internal Audit at 404-831-7946.