

July 15, 2025

Felecia A Green  
Deputy CIO  
Dept of Innovation & Technology  
Bobby Burgess Building  
3630 Camp Circle, Suite 301  
Georgia, 30032

**RE: 3rd Follow-Up – Management of Personally Identifiable Information (PII) - Audit Report No. 2019-009-IT**

Dear Ms. Green:

As required by DeKalb County, Georgia – Code of Ordinances/Organizational Act Section 10A-Independent Internal Audit (I), I have attached the Office of Independent Internal Audit's report on the status of management actions taken to address the findings contained in the referenced audit report. The conclusions in this follow-up report are limited to the status of the implementation and not the effectiveness of the completed action plans, which may be assessed in a future audit.

This report provides the results of our 3rd follow-up to verify the status of management action plans to address the remaining two findings.

Management is working to complete all the corrective action plans. Delays were due to staff and leadership changes in the Department of Innovation and Technology. The expectation is that Findings #2 and #3 will be completed by Q4 2025. We will follow up after these dates to verify the completion of the action plan(s).

**Figure 1 - Status of Management Actions Plans**

Finding No.	Report Findings	Status at 1st Follow-up December 08, 2022	Status at 2nd Follow-up June 18, 2024	Status at 3rd Follow-up July 02, 2025
1	The County Has Not Designated A Process Owner to Manage PII.	Closed		
2	There Were No Documented Policies and Procedures For The Management And Protection Of PII.	Partially Complete	Partially Complete	Partially Complete
3	The County Did Not Have an Awareness and Training Program For PII.	Partially Complete	Partially Complete	Partially Complete
4	The County Did Not Have an Incident Response Process in Place For PII	Closed		
5	There Were No Guidelines in Place for Managing PII With Third-Party Service Providers.	Closed		



## Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIVE

**FINAL**

Please contact me if you require additional information.

Sincerely,

*Lavois Campbell*

**Lavois Campbell, CFE, CISA, CIA, CGA-CPA**

Chief Audit Executive

**Cc:** 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  
Dr. G. Leah Davis, CEO's Chief of Staff  
Zachary L. Williams, Chief Operating Officer/ Executive Assistant  
William Jones, CIO, Department of Innovation & Technology  
Felecia Green, Deputy CIO, Department of Innovation & Technology

Dekalb County Government			
Office of Independent Internal Audit			
Date: July 02, 2025		Prepared by: Julie Ikioda	
Audit Findings Status Update Form			
Status Date	Report #	Report Title	
July 02, 2025	2019-009-IT	Audit of Management of Personally Identifiable Information (PII)	
Contact Person	Title	Phone No.	Email Address
Felecia Alston Green	Deputy CIO	470-330-5371	<a href="mailto:flalston@dekalbcountyga.gov">flalston@dekalbcountyga.gov</a>
Activity	Accountability	Schedule	
Follow Up	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
	Policies and Procedures	N/A	New Timeline - Q4, 2025.
Finding	Finding Detail		
No. 2			
Date 8/1/21			
Finding	There Were No Documented Policies And Procedures For The Management And Protection Of PII		
Recommendations	<p>We recommend that management develop, implement, and publish comprehensive County-wide PII policies and procedures. The policies and procedures should include, but not be limited to, the following topics:</p> <ul style="list-style-type: none"> <li>• Definition of PII.</li> <li>• Inventory of PII collected by the County.</li> <li>• Classification of PII.</li> <li>• Access rules for PII, especially electronic PII.</li> <li>• PII retention and disposal schedules and procedures.</li> <li>• Limitations on the collection, disclosure, maintenance, sharing, and use of PII.</li> <li>• Roles and responsibilities for collecting, processing, and protecting PII.</li> </ul>		
Management Response	<p>DoIT Management Agreement: <input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree</p> <p>Management agrees that policies and procedures need to be reviewed and enhanced. Having said that, there are policies and procedures under the auspices of DoIT that do govern electronic PII. DoIT abides by the National Institute of Standards and Technology Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) <a href="https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf">https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf</a>. There is also a DeKalb Cyber Incident Response procedure document that governs how the County responds to cyber-related incidents, which would include any compromise associated with PII data.</p> <p>Over the next 6 months, management will work on the coordinated enhancement of the governing documents and guidelines and create DeKalb County-specific PII references in policies and or create new ones as needed.</p> <p>Estimated Timeline to Implement Action Plan: Year-end 2021</p>		
Status Update-12 months	2022 Response:		
Open	DoIT policies which have over-reaching application to the entire DeKalb County government enterprise have been revised to specifically call out PII and shall be the basis by which other policies conform to. HR is working to complete its PII policy for HR related information by the middle of November. DoIT anticipates that the action plan will be completed by 3/31/2023.		
Management/Agency Assumes Risk			
X Partially Complete			
Complete Pending Verification by OIIA			
Closed			
OIIA Assessment - June 18, 2024	Management Status Update & OIIA Comments		
Open	Management Response:		
Management/Agency Assumes Risk	DoIT implemented a PII policy in 2022 and updated it in late 2023. The policies are also published to the Intranet. DoIT has also collaborated with the HR department, and training is provided both in New Employee Orientation as well as job specific training as needed, and addressed in finding 3.		
X Partially Complete			
Complete Pending Verification by OIIA			
Closed	<p>OIIA Comments</p> <p>DoIT provided a copy of the PII Compliance Policy last revised on June 18, 2024. The policy includes the topics recommended in the Audit report issued. It is anticipated that the PII procedures will be developed by end of July 2024.</p>		
OIIA Assessment - July 02, 2025	Management Status Update & OIIA Comments		
Open	Management Response:		
Management/Agency Assumes Risk	Currently under review with anticipated completion date of Q4 2025		
X Partially Complete			
Complete Pending Verification by OIIA	OIIA Comments:		
Closed	The finding is <b>Partially Complete</b> because the PII procedures have not been developed. Anticipated completion date is the Q4 2025.		

Dekalb County Government			
Office of Independent Internal Audit			
Date: July 2, 2025		Prepared by: Julie Ikioda	
Audit Findings Status Update Form			
Status Date	Report #	Report Title	
7/2/25	2019-009-IT	Audit of Management of Personally Identifiable Information (PII)	
Contact Person	Title	Phone No.	Email Address
Felecia Alston Green	Deputy CIO	470-330-5371	<a href="mailto:flalston@dekalbcountyga.gov">flalston@dekalbcountyga.gov</a>
Activity	Accountability	Schedule	
Follow Up	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
	Awareness and Training	N/A	New Timeline - Q4 2025
Finding		Finding Detail	
No.	3		
Date	8/1/21		
Finding		The County Did Not Have an Awareness And Training Program For PII	
Recommendations		<p>We recommend that management:</p> <ul style="list-style-type: none"> <li>• Develop a training plan and implementation approach.</li> <li>• Define roles and responsibilities for training, prerequisites for receiving access to PII, and ongoing training requirements. Further, we recommend training topics include, but not be limited to, the following:</li> <li>• The definition of PII.</li> <li>• Applicable privacy laws, regulations, and policies.</li> <li>• Restrictions on the collection, storage, and use of PII.</li> <li>• Roles and responsibilities for using and protecting PII.</li> <li>• Appropriate disposal of PII.</li> <li>• Recognition of security or privacy incidents involving PII.</li> <li>• Retention schedules for PII.</li> <li>• Roles and responsibilities in responding to PII-related incidents and reporting</li> </ul>	
Management Response		<p>DoIT Management Agreement: <input checked="" type="checkbox"/> Agree <input type="checkbox"/> Disagree</p> <p>Management will convene the team to prepare said documents. The principals will be the Human Resources, IT, and Finance Departments</p> <p>Estimated Timeline to Implement Action Plan: Q1 2022</p>	
Status Update-12 months		HR is developing countywide training that will include the involvement (roles and responsibilities) and policies of responding entities (IT, Purchasing, Finance/Risk Management and HR). Training will be conducted when all parties establish their policies. DoIT anticipates that the action plan will be completed by 3/31/2023.	
	Open		
	Management/Agency Assumes Risk		
X	Partially Complete		
	Complete Pending Verification by OIIA		
	Closed		
OIIA Assessment - June 18, 2024		Management Status Update & OIIA Comments	
	Open	Management Response:	
	Management/Agency Assumes Risk	HR has reassessed PII training needs and modified the approach as follows: HR will continue to provide the following PII training at New Employee Orientation (NEO) - what is PII, how it is stored; who needs to know and how to report a breach. Employees with PII access are required to complete confidentiality statements, which cover PII. Additionally, proper use of IT assets is explained. HR incorporates PII in the training for new payroll coordinators and occurs within 5 days of the role assignment. PII will be discussed at the 5/8/24 training for existing payroll coordinators. HIPAA training which may or may not be related to PII will be self-paced and released May 2024.	
X	Partially Complete		
	Complete Pending Verification by OIIA		
	Closed	<p><b>OIIA Comments</b></p> <p>1. DoIT has developed a training plan in the New Employee Orientation (NEO) handbook and a PII compliance policy. The policy defines roles and responsibilities for training, prerequisites for receiving access to PII, and ongoing training.</p> <p>2. The training topics in the NEO training handbook do not include retention schedules for PII, applicable privacy laws, regulations, and policies, restrictions on the collection, storage, and use of PII and roles and responsibilities for using and protecting PII.</p> <p>Updating the NEO training handbook involves HR and other key stakeholders. Anticipated completion date is December 31, 2024.</p>	
OIIA Assessment - July 02, 2025		Management Status Update & OIIA Comments	
	Open	Management Response:	
	Management/Agency Assumes Risk	Currently under review with anticipated completion date of Q4 2025	
X	Partially Complete		
	Complete Pending Verification by OIIA		
	Closed	<p>The finding is <b>Partially Complete</b> because the NEO training handbook that includes retention schedules for PII, applicable privacy laws, regulations, and policies, restrictions on the collection, storage, and use of PII and roles and responsibilities for using and protecting PII has not been updated.</p> <p><b>Anticipated completion date is the Q4 2025.</b></p>	