DeKalb County GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIV E

August 5, 2025

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

RE: 2nd Follow-up Report on Audit of Terminated and Transferred Employees Report No. IA-2021-007-IT

Dear Ms. Green:

As required by DeKalb County, Georgia – Code of Ordinances/Organizational Act Section10A-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 implementation status and not the effectiveness of the completed action plans, which may be assessed in a future audit.

Status of Audit Findings

Based on our review of management responses to the findings, the current status is outlined in the table below. Management is continuing to work on completing the corrective action plans and anticipates completing all actions by **the end of November 2025.**

Below is a summary of the status of management action plans.

Finding No.	Report Finding	Status of Management Action Plans as of June 4, 2024	Status of Management Action Plans as of July 31, 2025
1	County Policies and Procedures governing the Employee Termination and Transfer Process Need Improvement.	Partially Complete	**Partially Complete**
2	Untimely Deactivation of Application User Accounts after Employees are Terminated or Transferred.	Partially Complete	**Partially Complete**
3	Untimely Deactivation of Network Access for Terminated Employees.	Partially Complete	**Partially Complete**
4	Untimely Deactivation of Access from Email Distribution and Security Groups for Transferred Employees.	Partially Complete	**Partially Complete**
5	Periodic Reviews of Application User Account Access Were Not Performed.	Partially Complete	**Partially Complete**

Please contact me if you require additional information.

Sincerely,

Lavois Campbell

Lavois Campbell, CIA, CFE, CISA, 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

DeKalb County GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIV E

Dekalb County Government

Office of Independent Internal Audit

Date: 31 July, 2025 **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title		
7/31/25	IA-2021-007-IT	Audit of Terminated and Transferred Employees		
Contact Person	**Title**	**Phone No.**	**Email Address**	
Felecia Alston Green	Deputy CIO	470-330-5371	flalston@dekalbcountyga.gov	
Activity	**Accountability**		**Schedule**	
Follow-up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**	
	Policies and Procedure	**N/A**	**New Timeline - End of Nov 2025.**	

Finding		**Finding Detail**
No.	**1**	
Date	**May, 2023**	
Finding		**County Policies and Procedures governing the Employee Termination and Transfer Process Need Improvement**
Recommendations		We recommend that the DoIT and HR management should collaborate to establish countywide policies and procedures to include but not limited to the following: **1.** An "Access Control Policy" defines controls for disabling, removing, and modifying terminated and transferred employees' access to all County systems. **2.** An off-boarding checklist to serve as a guide for the termination and transfer process, including application and network user access. **3**. Stakeholders' roles and responsibilities relating to disabling and updating user access to applications and the County network. **4.** Timeframes for the deactivation or modification of user account access to applications and the County network when an employee is terminated or transferred. The timeframes may vary depending on if the termination is considered "friendly" or "unfriendly."4 **5.** Communication and training of County personnel on the updated policies, procedures, and tools. We discussed our observations and recommendations with HR management, who agreed and took proactive measures to address some of the recommendations and indicated readiness to collaborate with the user department and DoIT to further improve the process.
Management's Response		**DOIT** - Section 2.8 of the DoIT Security Policy, which was finalized on January 1, 2023, addresses Access Control and user security. With the implementation of CV360, Administrative controls have also been tightened to ensure the timely disablement of accounts. Processes are being shored up to ensure that Public Safety entities are more diligent in facilitating transfers in a timely manner. **HR** reviewed the DoIT Security Policy, January 1, 2023, and believes this policy adequately addresses access control and user security. With the implementation of CV360 processing of terminations has been expedited. The Off-boarding Checklist now includes the Property Inventory Form with links to the termination procedures on HR's intranet site and the CV360 training procedures for Payroll/Personnel Coordinators. The HRIS intranet page provides a timeframe for Payroll/Personnel Coordinators to submit terminations. The Off-boarding Checklist & Property Inventory Form should be used by Payroll/Personnel Coordinators for the transfer and separation of employees.

Finding # 1 Continued

OIIA Assessment - 12 months		Management Status Update & OIIA Comments
	Open	The January 1, 2023, Information Security Policy was reviewed. We noticed that the policy is still a draft that has not been approved. Section 2.8 of the DeKalb ISP states that County employees or contractors separating or terminating employment with DeKalb County Government shall have access to information systems and information revoked and the Employee Clearance Record must be completed. However, no timeframe was stated for the deactivation or modification of user account access to applications and the County network when an employee is terminated or transferred. According to DoIT, accounts are deactivated/modified immediately they are notified by the department/agency and the Information Security Policy will be approved by end of 3rd quarter 2024.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

OIIA Assessment - July 31, 2025		Management Status Update & OIIA Comments
	Open	**Management Response:** DoIT will have the Information Security Policy (ISP) updated within 30 days. The overall process, including necessary reviews and approvals, will take a minimum of four months. Please see the detailed project plan below. DoIT will provide monthly updates on the progress.
	Management/Agency Assumes Risk	
X	**Partially Complete**	
	Complete Pending Verification by OIIA	
	Closed	

Week	Activity
Week 1	Gather input from internal stakeholders (DoIT teams, security leads)
Week 2-3	Draft updated Information Security Policy
Week 4	Circulate draft to internal stakeholders for review
Week 5	Incorporate stakeholder feedback and finalize working draft
Week 6-7	Submit to OIIA for review and receive feedback
Week 8	Revise draft based on OIIA feedback
Week 9-12	Submit to Law Department for review (30–60 day window)
Week 13	Receive final comments and revise as needed
Week 14	Final internal review with OIIA and DoIT
Week 15-16	Submit to COO for final review and approval

OIIA Comments:
The finding is **Partially Complete** because the Information Security Policy (ISP) reflecting the timeline for deactivation of user access to applications and the County network have not been updated and approved.
Communication and training of County personnel on the updated policies, procedures should be effected when the policies and procedures are updated and approved. DoIT management has proposed completion date of **Nov 2025.**

DeKalb County GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIVE

Dekalb County Government

Office of Independent Internal Audit

Date: July 31, 2025 **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title
7/31/25	IA-2021-007-IT	Audit of Terminated and Transferred Employees

Contact Person	Title	Phone No.	Email Address
Felecia Alston Green	Deputy CIO	470-330-5371	flalston@dekalbcountyga.gov

Activity	Accountability		Schedule
	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
Follow-up	Application User Access	N/A	New Timeline - End of Nov 2025.

Finding		Finding Detail
No.	2	
Date	May, 2023	
Finding		**Untimely Deactivation of Application User Accounts after Employees are Terminated or Transferred.**
Recommendations		We recommend that DoIT management should collaborate with user departments to : 1. Provide guidance to the user departments and their application vendors to help ensure user departments establish procedures that ensure the dates of deactivation of the user account are tracked and periodically reviewed (refer to the recommendations for finding # 5). 2. Include user departments on the distribution list for termination and transfer reports or grant user departments the ability to generate the reports to help ensure the timely notification of termination or transfer of employees.
Management's Response		Departments/Agencies are responsible for ensuring that applications that they are responsible for the Administration of, have access control processes in place to ensure timely adjustments and/or removals and additions of access. **DoIT and HR will ensure that accountable department/agency administrators receive reports that impact access control status.**

OIIA Assessment - 12 months		Management Status Update & OIIA Comments
	Open	The January 1, 2023, Information Security Policy that will provide guidance was reviewed. The policy is still a draft and according to DoIT management, it will be approved by end of 3rd quarter 2024. DoIT provided a list of user departments that are on the distribution list to receive the termination and transfer reports to ensure the timely notification of termination or transfer of employees. New Timeline - End of 3rd quarter 2024.
	Management/Agency Assumes	
X	Partially Complete	
	Complete Pending Verification by	
	Closed	

OIIA Assessment - July 31, 2025		Management Status Update & OIIA Comments
	Open	**Management Response:** DoIT will have the Information Security Policy (ISP) updated within 30 days. The overall process, including necessary reviews and approvals, will take a minimum of four months. Please see the detailed project plan below. DoIT will provide monthly updates on the progress
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

Week	Activity
Week 1	Gather input from internal stakeholders (DoIT teams, security leads)
Week 2-3	Draft updated Information Security Policy
Week 4	Circulate draft to internal stakeholders for review
Week 5	Incorporate stakeholder feedback and finalize working draft
Week 6-7	Submit to OIIA for review and receive feedback
Week 8	Revise draft based on OIIA feedback
Week 9-12	Submit to Law Department for review (30–60 day window)
Week 13	Receive final comments and revise as needed
Week 14	Final internal review with OIIA and DoIT
Week 15-16	Submit to COO for final review and approval

OIIA Comments:
The finding is **Partially Complete** because the Information Security Policy (ISP) is currently under review hoping to be finalized by November of 2025.

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIVE

Dekalb County Government

Office of Independent Internal Audit

Date: July 31, 2025 **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title
7/31/25	IA-2021-007-IT	Audit of Terminated and Transferred Employees

Contact Person	Title	Phone No.	Email Address
Felecia Alston Green	Deputy CIO	470-330-5371	flalston@dekalbcountyga.gov

Activity	Accountability		Schedule
	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made
Follow-up	Network User Access	N/A	New Timeline - End of Nov 2025.

Finding		Finding Detail
No.	3	
Date	May, 2023	
Finding		**Untimely Deactivation of Network Access for Terminated Employees.**
Recommendations		We recommend that DoIT, HR, and user departments management should collaborate to: 1. Immediately deactivate the active network accounts identified during the audit for terminated employees as stated by best practices such as the NIST, PCI-DSS, and COBIT. 2. Confirm the status of the network accounts for terminated employees that did not appear on either the active or disabled network account status reports and immediately deactivate any active network accounts. 3. Take immediate action to help ensure the integrity and completeness of the network account active and disabled status reports. 4. Implement the updated policies and procedures noted in the recommendations for finding number one and ensure the procedure indicates the requirement for departments to timely transfer application responsibilities and data to another employee so as not to delay deactivating the network accounts for terminated employees.
Management's Response		**DoIT -** With the go-live of CV360 in January of 2022, more timely reports are being provided, and accounts are being deactivated/terminated more timely. DoIT and HR will continue to work with Departments/Agencies to remove exceptions to processes that have been requiring reinstatement of accounts for authorized business use but with no access being provided to the terminated employee. As legacy systems are decommissioned, these issues are becoming less frequent and will be eliminated. Also, the delays caused by certain departments/agencies not entering data into the system in a timely fashion is being addressed. **HR -** The recommended collaboration is in place, and HR concurs with DoIT's response. The DoIT January 1, 2023, Security Policy adequately addresses access control and user security. Additionally, the Off-boarding Checklist & Property Inventory Form includes a reminder for departments to manage or terminate system access. The updated form should provide increased awareness and compliance.

OIIA Assessment -12 months		Management Status Update & OIIA Comments
	Open	1. Deactivate the active network accounts identified during the audit for terminated employees as stated by best practices such as the NIST, PCI-DSS, and COBIT. **Implemented**
	Management/Agency Assumes	
X	Partially Complete	2. Confirm the status of the network accounts for terminated employees that did not appear on either the active or disabled network account status reports during the audit and immediately deactivate any active network accounts. **Implemented**
	Complete Pending Verification by	
	Closed	3. Take immediate action to help ensure the integrity and completeness of the network account active and disabled status reports. We sampled 2023 to test if actions have been taken. Work is in progress to fully resolve. **Partially implemented.** 4. Implement the updated policies and procedures noted in the recommendations for finding number one and ensure the procedure indicates the requirement for departments to timely transfer application responsibilities and data to another employee so as not to delay deactivating the network accounts for terminated employees. HR has updated the Off-boarding Checklist & Property Inventory Form. The updated Information Security policy was reviewed and we noted that it has not been approved. The updated policy and procedures are anticipated to be approved by the end of the third quarter of 2024.

Finding # 3 Continued

	OIIA Assessment - July 31, 2025
	Open
	Management/Agency Assumes Risk
X	Partially Complete
	Complete Pending Verification by OIIA
	Closed

Management Status Update & OIIA Comments

Management Response:

DoIT will have the Information Security Policy (ISP) updated within 30 days. The overall process, including necessary reviews and approvals, will take a minimum of four months. Please see the detailed project plan below. DoIT will provide monthly updates on the progress

Week	Activity
Week 1	Gather input from internal stakeholders (DoIT teams, security leads)
Week 2-3	Draft updated Information Security Policy
Week 4	Circulate draft to internal stakeholders for review
Week 5	Incorporate stakeholder feedback and finalize working draft
Week 6-7	Submit to OIIA for review and receive feedback
Week 8	Revise draft based on OIIA feedback
Week 9-12	Submit to Law Department for review (30–60 day window)
Week 13	Receive final comments and revise as needed
Week 14	Final internal review with OIIA and DoIT
Week 15-16	Submit to COO for final review and approval

OIIA Comments:

DoIT has deactivated network access for 14 of 15 terminated employees that were on the list at the time of 1st follow-up. Only 1 of 15 employees was noted on the list who is a current employee. Recommendation 3 is deemed to be **implemented.**

The finding is **Partially Complete** because the Information Security Policy (ISP) and the Procedures that specify the requirement for departments to timely transfer application responsibilities and data to another employee so as not to delay deactivating the network accounts for terminated employees have not been updated and approved. DoIT management has proposed completion date of Nov 2025.

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIVE

Dekalb County Government

Office of Independent Internal Audit

Date: July 31, 2025 **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title		
7/31/25	IA-2021-007-IT	Audit of Terminated and Transferred Employees		
Contact Person	**Title**	**Phone No.**	**Email Address**	
Felecia Alston Green	Deputy CIO	470-330-5371	flalston@dekalbcountyga.gov	
Activity	**Accountability**		**Schedule**	
Follow-up	Responsible Area	Repeat Finding	Anticipated Completion Date/Date Adjustments will be made	
	Email Distribution and Security Groups Access	N/A	New Timeline - End of Nov 2025.	

Finding		Finding Detail
No.	4	
Date	May, 2023	
Finding		**Untimely Deactivation of Access from Email Distribution and Security Groups for Transferred Employees.**
Recommendations		We recommend that the DoIT management collaborates with the management of the departments to: 1. Establish procedures and specify required timelines to help ensure the timely deactivation of transferred employees' access to the email distribution and security groups when no longer required. This should be aligned with the timelines indicated in the access control policy referenced in the recommendations to finding 1. 2. Implement a process to ensure complete and consistent data is captured and retained as per data retention practices.
Management's Response		All email lists and distribution lists are being cleansed as a function of the Active Directory modernization project. The reality of this finding is that though some people may not have been transferred in a timely fashion, the access that they have through the lists is usually quickly remedied when they need access to the group areas that they have been transferred to. This is most commonly found in public safety departments/agencies where people frequently rotate to new positions, sometimes as often as every six months.

OIIA Assessment -12 months		Management Status Update & OIIA Comments
	Open	The updated Information Security policies and procedures will specify required timelines for timely deactivating employees' access to email distribution and security groups. They are expected to be approved by the end of the third quarter of 2024.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

OIIA Assessment - July 31, 2025		Management Status Update & OIIA Comments
	Open	**Management Response:** DoIT will have the Information Security Policy (ISP) updated within 30 days. The overall process, including necessary reviews and approvals, will take a minimum of four months. Please see the detailed project plan below. DoIT will provide monthly updates on the progress.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

Week	Activity
Week 1	Gather input from internal stakeholders (DoIT teams, security leads)
Week 2-3	Draft updated Information Security Policy
Week 4	Circulate draft to internal stakeholders for review
Week 5	Incorporate stakeholder feedback and finalize working draft
Week 6-7	Submit to OIIA for review and receive feedback
Week 8	Revise draft based on OIIA feedback
Week 9-12	Submit to Law Department for review (30–60 day window)
Week 13	Receive final comments and revise as needed
Week 14	Final internal review with OIIA and DoIT
Week 15-16	Submit to COO for final review and approval

OIIA Comments:
The finding is **Partially Complete** because the Information Security Policy (ISP) and Procedures reflecting the timeline for deactivation of employees' access to email distribution and security groups have not been updated and approved. DoIT management has proposed completion date of Nov 2025.

DeKalb County GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIVE

Dekalb County Government

Office of Independent Internal Audit

Date: July 31, 2025 **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title		
7/31/25	IA-2021-007-IT	Audit of Terminated and Transferred Employees		
Contact Person	**Title**	**Phone No.**	**Email Address**	
Felecia Alston Green	Deputy CIO	470-330-5371	flalston@dekalbcountyga.gov	
Activity	**Accountability**	**Schedule**		
Follow-up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**	
	Application User Access Reviews	**N/A**	**New Timeline - End of Nov 2025.**	

Finding		Finding Detail
No.	5	
Date	May, 2023	
Finding		**Periodic Reviews of Application User Account Access Were not Performed.**
Recommendations		We recommend that the DoIT management coordinates with the user departments and HR management to: 1. Establish a standard operating procedure for the periodic review of users' access and roles on the departments' applications. The procedure should include but is not limited to: o The identification, roles, and responsibilities of the review managers conducting the review and other stakeholders. o The required reports needed for a complete review of the users. o The criteria, guidelines, and documentation required to be maintained to support the review. o The period, duration, and frequency of the review. o The procedures for addressing and validating recommendations made during the review. 2. Establish a procedure for routine training of the reviewing officers to ensure that accurate and appropriate application user access reviews are carried out. 3. Facilitate the review process by ensuring that departments' stakeholders (payroll coordinators and system administrators) have timely access to their department termination and transfer reports (refer to recommendations for finding 2).
Management's Response		**DoIT will request that departments/agencies conduct quarterly reviews of user accounts and access levels for those systems under their purview.** Though DoIT is happy to take the lead on coordinating, collaborating, and reminding – DoIT is NOT responsible NOR accountable for this function. Before the implementation of CV360, departments/agencies already had this capability and had received training on their respective systems from their vendor and, in some cases, from DoIT. DoIT will continue to share best practices and recommendations with departments/agencies. The implementation of CV360 has already made this process more timely and created better mechanisms for reporting and reminding.

Finding # 5 Continued

	OIIA Assessment -12 months	Management Status Update & OIIA Comments
	Open	DoIT provided a list of user departments that are on the distribution list to receive the termination and transfer reports to ensure the timely notification of termination or transfer of employees. It is anticipated that the updated User Access policies and procedures will be approved by the end of 3rd quarter 2024.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

	OIIA Assessment - July 31, 2025	Management Status Update & OIIA Comments
	Open	**Management Response:** DoIT will have the Information Security Policy (ISP) updated within 30 days. The overall process, including necessary reviews and approvals, will take a minimum of four months. Please see the detailed project plan below. DoIT will provide monthly updates on the progress
	Management/Agency Assumes Risk	
X	**Partially Complete**	
	Complete Pending Verification by OIIA	
	Closed	

Week	Activity
Week 1	Gather input from internal stakeholders (DoIT teams, security leads)
Week 2-3	Draft updated Information Security Policy
Week 4	Circulate draft to internal stakeholders for review
Week 5	Incorporate stakeholder feedback and finalize working draft
Week 6-7	Submit to OIIA for review and receive feedback
Week 8	Revise draft based on OIIA feedback
Week 9-12	Submit to Law Department for review (30–60 day window)
Week 13	Receive final comments and revise as needed
Week 14	Final internal review with OIIA and DoIT
Week 15-16	Submit to COO for final review and approval

OIIA Comments:

The finding is **Partially Complete** because the User Access Policies and Procedures have not been updated and approved. **DoIT management has proposed completion date of Nov 2025.**