DeKalb County
GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

June 7, 2024

Mr. John Matelski
Chief Information Officer
Dept of Innovation & Technology
Bobby Burgess Building
3630 Camp Circle, Suite 301
Georgia, 30032.

RE: Follow-up Report on Audit of Termination and Transfer of Employees - Report No. IA-2021-007-IT

Dear Mr. Matelski:

As required by DeKalb County, Georgia – Code of Ordinances/Organizational Act Section 10A – Independent Internal Audit (I), the Office of Independent Internal Audit has completed a follow-up of the audit noted above. I have attached the Office of Independent Internal Audit's report on the status of management actions 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 action plans, which may be assessed in a future audit.

Status of Audit Findings

Based on our review of management responses to the findings, we concluded that the five recommendations are Partially Completed. Management is continuing to work on completing the corrective action plans, which include updating the Information Security Policy and Standard Operating Procedures. They are expected to **be completed by the end of the third quarter of 2024**. We will follow up after that date to verify the completion of the action plan(s).

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

Please contact me if you require additional information.

Sincerely,

Lavois Campbell

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

cc . Michael L. Thurmond, Chief Executive Officer
Robert Patrick, Board of Commissioners District 1
Michelle Long Spears, Board of Commissioners District 2
Steve Bradshaw, Board of Commissioners District 4
Mereda Davis Johnson, Board of Commissioners District 5
Ted Terry, Board of Commissioners District 6
Gloria G. Gray, Chairperson, Audit Oversight Committee
Adrienne T. McMillion, Vice-Chairperson, Audit Oversight Committee
Lisa Earls, Chairperson pro-tem, Audit Oversight Committee
Tanja Christine Boyd-Witherspoon, Audit Oversight Committee
Zachary L. Williams, Chief Operating Officer/ Executive Assistant
Vivian Ernstes, County Attorney
La'Keitha D. Carlos, CEO's Chief of Staff
Kwasi K. Obeng, Chief of Staff, Board of Commissioners

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government

Office of Independent Internal Audit

Date: May 31, 2024. **Prepared by: JI**

Audit Findings Status Update Form

Status Date	**Report #**	**Report Title**
May 31, 2024.	IA-2021-007-IT	Audit of Terminated and Transferred Employees

Contact Person	**Title**	**Phone No.**	**Email Address**
John Matelski	Chief Innovation & Information Officer	**404-371-6210**	jmatelski@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 3rd quarter 2024.**

Finding		**Finding Detail**
No.	1	
Date	May, 2023	

Finding	**County Policies and Procedures Governing the Employee Termination and Transfer Process Need Improvement**
Recommendation	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 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.

Status Update		
	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 the 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 after they are notified by the department/agency, and the Information Security Policy will be approved by the end of the 3rd quarter of 2024.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

DeKalb County
GEORGIA

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government

Office of Independent Internal Audit

Date: May 31, 2024. **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title
May 31, 2024.	IA-2021-007-IT	Audit of Terminated and Transferred Employees

Contact Person	Title	Phone No.	Email Address
John Matelski	Chief Innovation & Information Officer	**404-371-6210**	jmatelski@dekalbcountyga.gov

Activity	Accountability	Schedule	
Follow Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Application User Access	**N/A**	**3rd Quarter 2023** **New Timeline - End of 3rd quarter 2024.**

Finding		Finding Detail
No.	2	
Date	May, 2023	
Finding		**Untimely Deactivation of Application User Accounts after Employees are Terminated or Transferred.**
Recommendation		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 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.

Status Update		
	Open	The January 1, 2023, Information Security Policy that will provide guidance was reviewed. The policy is still a draft, but according to DoIT management, it will be approved by the end of the third quarter of 2024. DoIT provided a list of user departments on the distribution list to receive the termination and transfer reports, ensuring timely notification of termination or transfer of employees.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government			
Office of Independent Internal Audit			
Date: May 31, 2024.		**Prepared by: JI**	
Audit Findings Status Update Form			
Status Date	**Report #**	**Report Title**	
May 31, 2024.	IA-2021-007-IT	Audit of Terminated and Transferred Employees	
Contact Person	**Title**	**Phone No.**	**Email Address**
John Matelski	Chief Innovation & Information Officer	**404-371-6210**	jmatelski@dekalbcountyga.gov
Activity	**Accountability**	**Schedule**	
Follow Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Network User Access	**N/A**	**New Timeline - End of 3rd quarter 2024.**

Finding		**Finding Detail**
No.	3	
Date	May, 2023	
Finding		**Untimely Deactivation of Network Access for Terminated Employees.**
Recommendation		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 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.

Status Update		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** 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** 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 whether actions have been taken. Work is in progress to fully resolve this. It is partially **implemented.** 4. Implement the updated policies and procedures noted in the recommendations for finding number one and ensure the procedure indicates the department's requirement to transfer application responsibilities and data to another employee in a timely manner 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.
	Open	
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUT IV E

FINAL

DeKalb County Government				
Office of Independent Internal Audit				
Date: May 31, 2024.			**Prepared by: JI**	
Audit Findings Status Update Form				
Status Date	**Report #**	**Report Title**		
May 31, 2024.	IA-2021-007-IT	Audit of Terminated and Transferred Employees		
Contact Person	**Title**		**Phone No.**	**Email Address**
John Matelski	Chief Innovation & Information Officer		**404-371-6210**	jmatelski@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 3rd quarter 2024.**

Finding		**Finding Detail**
No.	4	
Date	May, 2023	
Finding		**Untimely Deactivation of Access from Email Distribution and Security Groups for Transferred Employees.**
Recommendation		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 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.
Status Update		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.
	Open	
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	

Office of Independent Internal Audit

LAVOIS CAMPBELL, CHIEF AUDIT EXECUTIVE

FINAL

DeKalb County Government

Office of Independent Internal Audit

Date: May 31, 2024. **Prepared by: JI**

Audit Findings Status Update Form

Status Date	Report #	Report Title
May 31, 2024.	IA-2021-007-IT	Audit of Terminated and Transferred Employees

Contact Person	Title	Phone No.	Email Address
John Matelski	Chief Innovation & Information Officer	**404-371-6210**	jmatelski@dekalbcountyga.gov

Activity	Accountability		Schedule
Follow Up	**Responsible Area**	**Repeat Finding**	**Anticipated Completion Date/Date Adjustments will be made**
	Application User Access	**N/A**	**New Timeline - End of 3rd quarter 2024.**

Finding		Finding Detail
No.	5	
Date	May, 2023	
Finding		**Periodic Reviews of Application User Account Access Were not Performed.**
Recommendation		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 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.

	Status Update	
	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 information security policy (ISP) will be approved and the standard operating procedures established by the end of 3rd quarter 2024.
	Management/Agency Assumes Risk	
X	Partially Complete	
	Complete Pending Verification by OIIA	
	Closed	