OFFICE OF INDEPENDENT INTERNAL AUDIT

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

May 2023

DeKalb County Government

AUDIT OF THE TERMINATION AND TRANSFER OF EMPLOYEES PROCESS

COUNTY APPLICATIONS AND NETWORK

FINAL REPORT

Audit Report No. IA-2021-007-IT

The page was intentionally left blank.

OFFICE OF INDEPENDENT INTERNAL AUDIT

DeKalb County GEORGIA

Lavois Campbell
Chief Audit Executive

AUDIT OF TERMINATION AND TRANSFER OF EMPLOYEES REPORT NO. IA-2021-007-IT

FINAL

HIGHLIGHT SUMMARY

Why We Performed the Audit

In accordance with the Office of Independent Internal Audit (OIIA) Annual Audit Plan, we conducted a Countywide performance audit of the Termination and Transfer of Employees Process. The purpose of the audit was to evaluate the effectiveness of the procedures and processes specifically **related to the deactivation or modification of terminated and transferred employees' user access to the County network and applications**.

The departments in focus utilize various applications to process the County residents' sensitive data that require optimized data security. The selected applications are used to process the County's criminal justice information, maintain the County's vehicle and equipment records, record and process residents' incident and emergency information, maintain responders' training records, process geographical information, process building and development permits, business licenses, trade licenses, and code enforcement information. The timely deactivation or modification of terminated and transferred employees' user access to these applications and the County network is critical to the security of sensitive citizens' information. Gaps and weaknesses in the controls would be an opportunity for unauthorized access and breach of data that could result in operational, reputational, regulatory, and or financial loss to the County.

According to a recent *Chief Information Officers' Leadership insights report*, 20% of organizations experienced data breaches by former employees. Of those, 47% admitted that ex-employees have been responsible for more than 10% of all their data breaches[1].

How We Performed the Audit

The audit focused on the County Termination and Transfer of Employees process from January 1, 2020, through December 31, 2021. Our methodology included, but was not limited to, the following:

- Reviewed the policies and procedures relating to the Termination and Transfer of Employees process and related best practices.
- Selected and tested a sample of Termination and Transfer of Employees activities.
- Reviewed supporting documentation and information.
- Interviewed appropriate County personnel.

Background

DeKalb County and its various departments and agencies provide essential services to its citizens. To provide these services the departments utilize various applications to collect, record and process the County resident's sensitive data and personally identifiable information (PII) to provide these services. The departments and associated applications included in this audit were selected based on the sensitive information that is involved in the various services provided. In addition, the administration of user access for the selected applications is managed primarily by the department personnel, with limited support from the Department of Innovation and Technology (DoIT). The selected applications are Hansen (for asset management), Odyssey (for case management), Image Trend (for incident reporting), Vector Solution (training records management system), Projectdox (for managing plan review process), Faster (for managing inventory of equipment and County fleet vehicles), and the geographical information services (GIS) system that captures stores, analyzes, manages, and presents various geographical data.

What We Found

The audit noted that the departments use the Human Resource (HR) Administrative Policies and Procedures to guide the termination and transfer employee process. The following opportunities to strengthen controls were also identified.

Audit Findings	Results
1. County Policies and Procedures Governing the Employee Termination and Transfer Process Need Improvement	🟨
2. Untimely Deactivation of Application User Accounts After Terminating or Transferring Employees.	🟥
3. Untimely Deactivation of Network Access for Terminated Employees.	🟥
4. Untimely Deactivation of Access from Email Distribution and Security Groups for Transferred Employees.	🟥
5. Periodic Reviews of Application User Account Access is Not Performed.	🟥

🟩	No exceptions were noted.
🟨	Recommendation to enhance internal controls.
🟥	Internal control exceptions noted require action.

What We Recommend

We recommend that the Program Areas, HR, and DoIT managements collaborate to address the control process deficiencies identified in this report.

How Management Responded

Management agrees with the report's findings and is working on corrective actions to address the control gaps.

[1] https://www.cioinsight.com/security/ex-employees-still-cause-data-breaches/

TABLE OF CONTENTS

BACKGROUND AND INTRODUCTION

DeKalb County, through its various departments and agencies, provides essential services to its citizens, such as public utilities, economic development, environmental and natural resource management, enforcing compliance with codes established to protect public health, safety, fire, and emergency medical protection, zoning, business license activities, integrated geographical information services (GIS), and maintenance of the County's vehicle fleet, and provide legal representation to citizens unable to afford an attorney. To provide these services, the departments utilize various applications to collect, record and process the County resident's sensitive data and personally identifiable information (PII)[2]. Therefore, the security of the applications, including user access management, is critical to safeguarding residents' sensitive information.

Why We Performed the Audit

The audit was part of the OIIA audit plan because of the PII, such as name, date of birth, address, driver's license, mobile or email, and social security number, managed by the applications used in providing County services. The timely deactivation and modification of terminated and transferred employees on these applications and the County network is critical to the security of citizens' sensitive information. According to the Chief Information Officers' Leadership Insights (CIO Insight) report, 20% of organizations experienced data breaches by former employees. Of those, 47% admitted that ex-employees have been responsible for more than 10% of all their data breaches. [3]

To mitigate the risk of unauthorized access and improper use of data, adequate logical access controls (authentication and authorization) should be in place to ensure that user access is appropriate, given the current roles and responsibilities. Gaps and weaknesses in the controls would be an opportunity for unauthorized access to data or data breaches which could result in reputational, operational, and regulatory loss to the County.

Our Scope and Objectives

This audit aimed to assess the effectiveness of the internal controls over the access to data and information processed by applications and identify vulnerabilities that could be exploited if user accounts are not de-provisioned (i.e., deactivated) when no longer required. The Administration of application user accounts and access to many of these applications is managed by the departments with limited support from DoIT. In addition, access to some of these applications requires access to the County network, which DoIT manages. The departments also collaborate with Human Resources and Merit System Department (HR) and DoIT when employees are terminated or transferred.

The main document that guides the termination and transfer of employee process is the HR Administrative Policies & Procedures and other documents like the Personnel Action (PA2) and Inventory and Separation Notice forms. Together these documents guide the following:

[2] PII is any information that can be used to distinguish or trace an individual's identity or linkable to an individual's personal, medical, educational, financial, and employment information.

[3] https://www.cioinsight.com/security/ex-employees-still-cause-data-breaches/

- Deactivation of an employee's access to the company's network and computer systems upon the termination of their employment.
- Modifying employee access upon transfer to another department/area within the organization.

During the planning phase of the audit, a sample of six (6) departments was selected as the focus of this audit. These departments manage access to applications that process sensitive information of County employees and citizens, including address, name, social security/tax number, email/phone number, insurance details, social media accounts, inventory data of vehicles, repairs & maintenance. The table below indicates the departments and the respective applications considered in this audit:

	Department	Key Applications Used
1	Code Compliance	Hansen and GIS app.
2	Fleet Management Division	Faster
3	Fire Rescue	Vector Solutions and Image Trend
4	Geographic Information Systems (GIS)	Hansen
5	Planning & Sustainability	Hansen and Projectdox
6	Public Defender	Odyssey (DeKalb County State Court manages application user accounts)

Our audit procedures included discussions with key stakeholders and management staff, review of policies and procedures, and tests of transactions to assess the effectiveness of the controls to help ensure the deactivation or modification of application and network user accounts of terminated or transferred employees.

AUDIT RESULTS

We noted that the departments utilized the HR Administrative Policies and Procedures to guide the termination and transfer process. The audit identified opportunities for strengthening the processes for deactivating or modifying user access for employees terminated or transferred who no longer required access to the application and/or the County network. While we did not identify unauthorized user account access, the identified user access control deficiencies significantly increased the risks of unauthorized access to the County network, applications, sensitive data, and personally identifiable information (PII). The detailed findings and corresponding recommendations are outlined in this report.

Finding 1: County Policies and Procedures Governing the Employee Termination and Transfer Process Need Improvement.

We discussed, with personnel in the user departments, HR, and DoIT, the policies and procedures governing the County's employee termination and transfer processes. We reviewed the available County policies and procedures governing the general termination process, including the HR Administrative Policies and Procedures, the PA2 form, the inventory form, and other related documents. We also reviewed better practices for the employee termination and transfer process. We determined that existing policies and procedures did not include:

- Countywide high-level requirements specify how user access is managed, who may access information (applications and county network), and under what circumstances.
- Roles and responsibilities relating to disabling and updating user access when employees are terminated or transferred.
- The steps to be performed (an off-boarding checklist) when an employee terminates or transfers, including requirements for user application and network access.
- The timelines for removing or modifying users' access to all applications and the County network when employees are terminated or transferred.

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:

- An "Access Control Policy" defines controls for disabling, removing, and modifying terminated and transferred employees' access to all County systems.
- An off-boarding checklist to serve as a guide for the termination and transfer process, including application and network user access.
- Stakeholders' roles and responsibilities relating to disabling and updating user access to applications and the County network.
- Timeframes for deactivating or modifying 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]
- 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 recommendations before the finalization of our report.

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	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	Complete but ongoing enhancements are being reviewed to ensure departmental/agency compliance.

[4] NIST Special Publication 800-53: Personnel Termination PS-4.

Management Response (HR Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	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.	Complete, and will continue to review and include enhancements as necessary.

Finding 2: Untimely Deactivation of Application User Accounts after Terminating or Transferring Employees.

Through discussions, we determined that user department management had not documented its procedures for deactivating users' accounts on applications when the employee was terminated or transferred and no longer required access. Our audit verified if application user accounts for terminated or transferred employees were deactivated in a timely manner. We compared an HR-provided listing of County terminated and transferred employees during our audit period against the population of active user accounts for the seven applications in the scope of this review. We identified 124 user accounts in seven applications that were not deactivated as of the date of our audit, 12 to 28 months after the employees were terminated or transferred, as shown in Table 1. These accounts have since been deactivated.

Table 1 – Number of application user accounts active at the time of our audit**,** months after the termination or transfer of employees.

Department	Application	
	Hansen	**GIS**
Code Compliance	10 accounts active ≥ 28 months	20 accounts active ≥ 28 months

Department	Application	
	Hansen	**Projectdox**
Planning & Sustainability	7 accounts active ≥12 months	17 accounts active ≥12 months

Department	Application	
	Vector Solution	**Image Trend**
Fire Rescue	29 accounts active ≥12 months	26 accounts active ≥12 months

Department	Application	
	Odyssey*	
Public Defender	15 accounts active ≥12 months	

*The DeKalb County State Court manages the user access to this Odyssey application.

Furthermore, we selected samples of inactive application user accounts to determine if the accounts were deactivated timely. We determined that user accounts were not deactivated in a timely manner from the date of the employee's termination or transfer. In addition, we could not verify the timeliness of the deactivation of some application user accounts for GIS, Projectdox, and Faster because the deactivation date was not cited in the reports provided. See Table 2 for details.

Table 2 - Sample of application user accounts, which were deactivated *before* our audit, but were not deactivated timely, 51 days to more than 675 days after the employees were terminated or transferred.

Department	Application	
	Hansen	**GIS**
Code Compliance	1 of 5 accounts active ≥ 51 days.	1 of 1 deactivation timeline could not be validated.

Department	Application	
	Hansen	**ProjectDox**
Planning & Sustainability	3 of 5 accounts active ≥ 235 days.	3 of 3 deactivation timelines could not be validated.

Department	Application	
	Vector Solution	**Image Trend**
Fire Rescue	22 of 26 accounts active ≥ 675 days	19 of 20 accounts active ≥ 487 days

Department	Application
	Faster
Fleet	2 of 2 deactivation timelines could not be validated.

One contributing factor to the untimely user account deactivation was the timeliness of notification provided, by the user department (UD) of employees' termination and transfer, to HR and the UD application administrators. We selected a sample of terminated and transferred employees. We compared the effective dates with the date HR and the application administrators were notified. We determined that HR personnel and the application administrators were not notified timely of employee termination. For example, we noted that the HR department was not notified until 4 -15 days after the effective termination of 15 of 25 (60%) Fire Rescue employees. The HR termination training guide indicates that HR should be notified, by the user department, within 1 - 3 business days of the effective date of the employee's termination.

For other departments, Planning & Sustainability and Code Compliance, the timeliness of user department notification of employees' termination and transfer to HR and the UD application administrators could not be verified as supporting documentation was not provided.

Recommendation:

We recommend that DoIT management should collaborate with user departments to:

- Provide guidance to the user departments and their application vendors to help ensure they establish procedures that ensure the date of deactivation of the user account is tracked and periodically reviewed (refer to the recommendations for finding # 5).

- 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 (DoIT Management):

Management Agreement	***Description of Management's Action Plan to Address Finding***	***Estimated Timeline to Implement Action Plan***
☒ **Agree** ☐ **Disagree**	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.	3rd Quarter 2023

Finding 3: Untimely Deactivation of Network Access for Terminated Employees.

During the audit, we reviewed the procedures for deactivating the network access of terminated employees. We noted that there were no countywide documented procedures for the process.

Additionally, we reviewed the HR-provided report of terminated users for the audit period from January 2020 to December 2021. We compared it with the list of active network accounts and the list of deactivated network accounts. We determined that some County network accounts were not deactivated timely for the departments in scope. Specifically, we observed the following:

- 18 of 391 (4.6%) terminated employees' user network accounts were still active at the time of the audit (11 - 29 months after the effective termination dates). These accounts have since been deactivated.
- 136 of 391 (34.7%) terminated employees' network accounts were not deactivated timely (4 – 93 days after the effective termination date).
- 197 of 391 (50.3%) terminated employees were neither on the list of disabled nor the list of active network accounts, so we could not verify if the network accounts were disabled or active. We were informed that some of the records not provided were purged based on storage capacity management parameters used.
- 40 of 391 (10.2%) terminated employees' network accounts were deactivated timely from the network.

Additionally, we noted that for 17 terminated employees, their network and application user accounts were not deactivated in a timely manner (4 – 915 days after effective termination dates).

DoIT stated that requests from user departments contributed to some of the untimely deactivations of the terminated employees on the County network. User departments requested that DoIT not deactivate some network accounts or reactivate previously deactivated network accounts of terminated employees. The rationale for the requests included a need to maintain access to some applications and data until the data and responsibilities can be transferred to another employee. DoIT informed us that, though not deactivated, the password for the network accounts of terminated employees was changed to prevent the risk of access by the former employee. However, the risk of unauthorized access to the network, applications, and data by individuals aware of the new passwords existed. Also, we could not verify the password changes as the logs of the changes were not provided.

Recommendation:

We recommend that DoIT, HR, and user departments management should collaborate to:

- 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.
- 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.
- Take immediate action to help ensure the integrity and completeness of the network account active and disabled status reports.
- 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 Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	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.	Complete but ongoing enhancements are being reviewed to ensure departmental/agency compliance.

Management Response (HR Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	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.	Complete, and will continue to review and include enhancements as necessary.

Finding 4: Untimely Deactivation of Access from Email Distribution and Security Groups for Transferred Employees.

We reviewed the procedures for removing transferred users from their previous email distribution and security groups to the new email distribution and security groups. Security groups are used for managing access rights and permissions to resources such as network drives and SharePoint sites in an organization, while distribution groups are used for sending email notifications that are specific/unique to a group of people in an organization. We observed that access to security groups and email distribution groups was not modified in a timely manner when an employee was transferred and no longer required access. Specifically, we observed the following:

Security Group

- 4 of 16 (25%) transferred employees' access to their security groups was not modified in a timely manner (9 - 144 days after effective transfer dates).
- 2 of 16 (12.5%) transferred employees were not identified on the security groups list, so we could not determine how timely their access was modified.
- We could not verify how timely 6 of 16 (37.5%) transferred employees were removed from the security groups because the removal dates were not provided.
- 4 of 16 (25%) transferred employees' access to their security groups was modified timely.

Email Distribution Group

- 1 of 16 (6.3%) transferred employees' access to their former email distribution group was not modified in a timely manner (55 days after the effective transfer date).
- 8 of 16 (50%) transferred employees were not identified on the distribution groups list.
- We could not verify how timely 6 of 16 (31.3%) transferred employees were removed from the distribution groups because the removal dates were not provided.
- 1 of 16 (12.5%) transferred employees' access to their former email distribution groups was modified timely.

We were informed that some of the records not provided were archived or purged based on storage capacity management parameters used. However, we noted inconsistencies in the purging process, as some old and new records were purged within the same period.

Recommendation:

We recommend that the DoIT management collaborates with the management of the departments to:

- 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 needed. This should be aligned with the timelines indicated in the access control policy referenced in the recommendations to finding 1.
- Implement a process to ensure complete and consistent data is captured and retained as per data retention practices.

Management Response (DoIT Management):

Management Agreement	*Description of Management's Action Plan to Address Finding*	*Estimated Timeline to Implement Action Plan*
☒ **Agree** ☐ **Disagree**	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.	3rd Quarter 2023

Finding 5: Periodic Reviews of Application User Account Access Were Not Performed.

We interviewed the management of the user departments in scope. We determined that documented procedures for the periodic review and validation of users' account access, roles, and responsibilities for the applications did not exist.

Furthermore, the management of two of the six departments in scope (Fire Rescue and GIS) confirmed that they do not perform periodic reviews of application user account access.

We evaluated the current processes used by three departments, Code Compliance, Planning & Sustainability, and Fleet Management, to conduct periodic reviews of application user account access and observed that there were no documented evidence reviews to show that:

- The periodic reviews were performed and completed for the Hansen, Projectdox application, and GIS applications.
- Any recommendations from the review were implemented. For example, in Planning & Sustainability and Code Compliance departments, management stated that changes were not made for employees with inappropriate access to the Hansen and GIS applications.

Recommendation:

We recommend that the DoIT management coordinates with the user departments and HR management to:

- Establish a standard operating procedure for periodically reviewing users' access and roles on the departments' applications. The procedure should include but is not limited to:
  - The identification, roles, and responsibilities of the review managers conducting the review and other stakeholders.
  - The required reports needed for a complete review of the users.
  - The criteria, guidelines, and documentation required to be maintained to support the review.
  - The period, duration, and frequency of the review.
  - The procedures for addressing and validating recommendations made during the review.
- Establish a procedure for routine training of the reviewing officers to ensure that accurate and appropriate application user access reviews are carried out.
- 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 Management):

Management Agreement	***Description of Management's Action Plan to Address Finding***	***Estimated Timeline to Implement Action Plan***
☒ **Agree** ☐ **Disagree**	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.	3rd Quarter 2023

APPENDICES

Appendix I – Purpose, Scope, and Methodology

Purpose

The purpose of the audit was to evaluate the effectiveness of the procedures and processes specifically related to the disabling and updating of terminated and transferred employees' access to County applications and networks.

This involved:

- Assess the effectiveness of the policies and procedures related to the termination and transfer of employees' processes.
- Determine if terminated employees' access is removed timely from key applications and the County network and if transferred employees' access is modified upon transfer.
- Determine whether user access reviews are performed periodically by management.

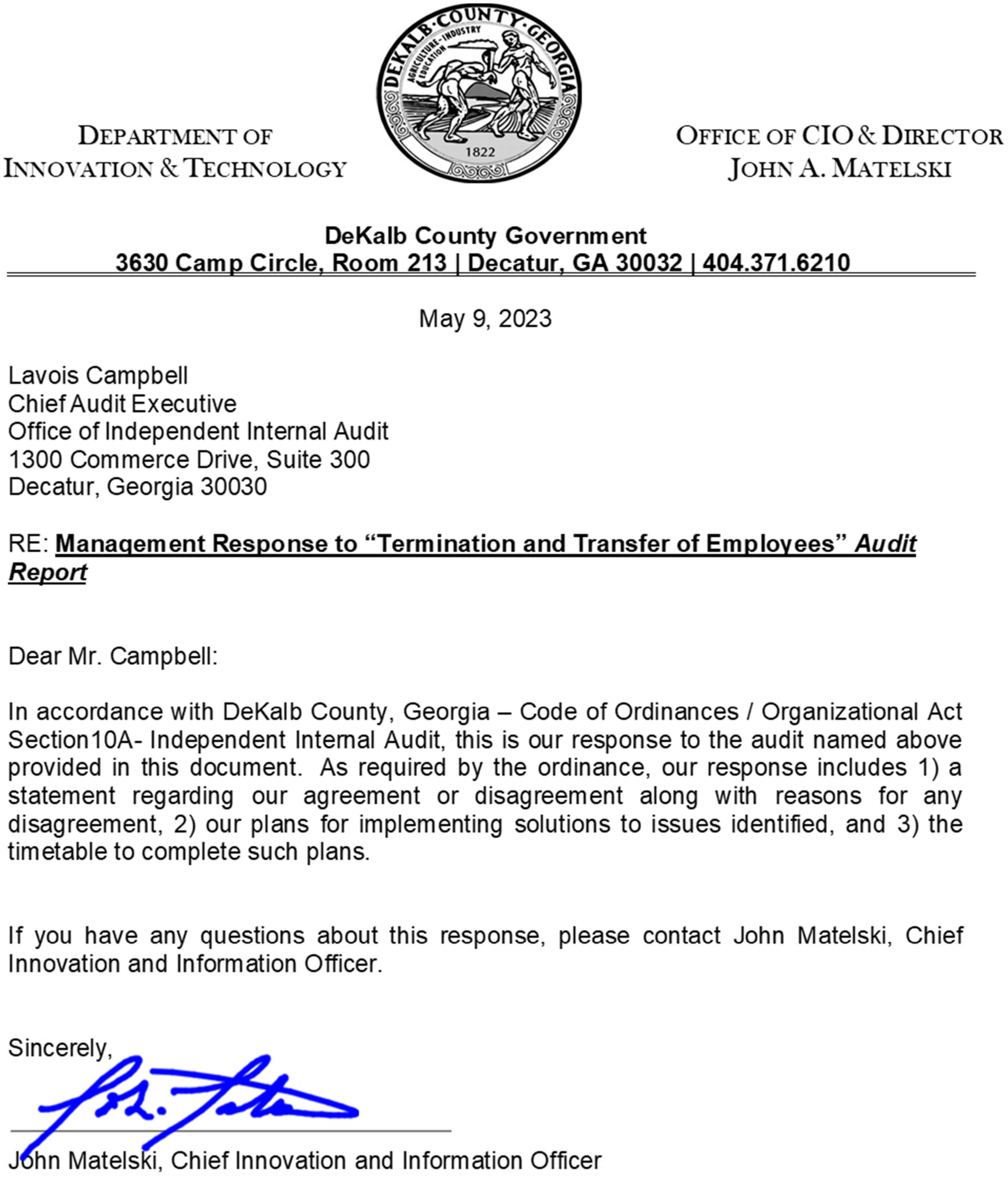
Scope and Methodology:

The scope of our audit focused on the termination and transfer of employees' activities from January 1, 2020, to December 31, 2021.

Our methodology included but was not limited to the following:

- Reviewed the policies and procedures relating to the Termination and Transfer of Employees process and related best practices.
- Selected and tested a sample of Termination and Transfer of Employees activities.
- Reviewed supporting documentation and information.
- Interviewed appropriate County personnel.

Appendix II – Management Response



DEPARTMENT OF
INNOVATION & TECHNOLOGY

OFFICE OF CIO & DIRECTOR
JOHN A. MATELSKI

DeKalb County Government
3630 Camp Circle, Room 213 | Decatur, GA 30032 | 404.371.6210

May 9, 2023

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

RE: **Management Response to "Termination and Transfer of Employees" *Audit Report***

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 John Matelski, Chief Innovation and Information Officer.

Sincerely,

John Matelski, Chief Innovation and Information Officer

Appendix III – Definitions and Abbreviations

Acronyms and Abbreviation

DoIT: Department of Innovation and Technology**.**

HR: Human Resources.

PCI-DSS: Payment Card Industry Data Security Standard.

DOL: Department of Labor.

PA2: Personnel Action Form.

PII: Personally Identifiable Information.

OIIA: Office of Independent Internal Audit.

COBIT: Control Objectives for Information and related Technology.

Key Definitions

Hansen: Hansen is an Asset Management System used by the Planning and Sustainability department. The system was known as Hansen until it was purchased by Infor in 2007 and renamed Infor Hansen. In 2013 it was rebranded as Infor Public Sector Asset Management Tools.

GIS app: A geographic information system (application) that captures, stores, analyzes, manages, and presents all types of geographical data.

Odyssey: A case management application designed to streamline the case and document workflow, financial assessments and collections, calendars, and caseload management.

Vector Solutions: A training records management system used by the Fire Rescue department.

Image Trend: A record management system for incident reporting at the Fire Rescue department.

Faster: A fleet system for maintenance and repairs used primarily to manage inventory (vehicles, pieces of equipment, parts, labor, repairs & maintenance) of the fleet.

Projectdox: A system designed for plan review process management that provides ease, reviewer efficiency, and greater process insight analytics.

CV360: A CloudVergent360 (CV360) Oracle Cloud HCM system was developed to provide DeKalb County users with a more streamlined and user-friendly method to access and update HR information.

De-provisioning: An access management practice of removing or deactivating user access to applications and data.

Terminated Employees: Employees whose employment with the County has ended either voluntarily or involuntarily.

Transferred Employees: Employees who transferred between departments within the County.

Security group: A group created in an organization to manage access permissions for all users on a department's folder.

Distribution group: A group created in an organization to enable a group of recipients in a specified department or unit to send and receive email messages related to events or activities in that department.

DISTRIBUTION

Action Official Distribution:

John Matelski, Chief Information Officer and Director of Innovation and Technology

Benita Ransom, Director, Human Resources & Merit System Department

Statutory Distribution:

Michael L. Thurmond, Chief Executive Officer

Robert Patrick, Board of Commissioners District 1

Michelle Long-Spears, Board of Commissioners District 2

Larry Johnson, Board of Commissioners District 3

Steve Bradshaw, Board of Commissioners District 4

Mereda Davis Johnson, Board of Commissioners District 5

Ted Terry, Board of Commissioners District 6

Lorraine Cochran-Johnson, Board of Commissioners District 7

Lisa Earls, Chairperson, Audit Oversight Committee

Gloria G. Gray, Vice-Chairperson, Audit Oversight Committee

Tanja Christine Boyd-Witherspoon, Pro-Tem, Audit Oversight Committee

Adrienne T. McMillion, Audit Oversight Committee

Harold Smith, Jr., Audit Oversight Committee

Information Distribution:

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

Timothy Hardy, Deputy Director, Code Compliance Administration

Cedric Hudson, Director (Interim), Planning & Sustainability

Darnell Fullum, Chief of Fire and Rescue, Fire Rescue

Stacy Grear, Director, GIS Department

Robert Gordon, Deputy Director, Fleet Management

PROJECT TEAM

This report was submitted by:

Julie Ikioda　　　　05/26.2023

Julie Ikioda, CISA, PMP
IT Internal Auditor, Senior
Office of Independent Internal Audit

Date

This report was reviewed by:

Rubby Ibe-Ikechi　　　　5/26/2023

Rubby A. Ibe-Ikechi, CISA, ISO/IEC 27001 LA
IT Audit Manager
Office of Independent Internal Audit

Date

The report was approved by:

Lavois Campbell　　　　5/30/2023

Lavois Campbell, CIA, CISA, CFE, CGA-CPA
Chief Audit Executive
Office of Independent Internal Audit

Date

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.