CITY AUDITOR'S OFFICE

CITY OF ATLANTA

PERFORMANCE AUDIT:

Offboarding

October 2, 2025
Project No. 25.06

www.atlaudit.org

CITY OF ATLANTA

AMANDA NOBLE
City Auditor
anoble@atlantaga.gov

STEPHANIE JACKSON
Deputy City Auditor
sjackson@atlantaga.gov

CITY AUDITOR'S OFFICE
68 MITCHELL STREET SW, SUITE 12100
ATLANTA, GEORGIA 30303-0312
http://www.atlaudit.org
(404) 330-6452
FAX: (404) 658-6077

October 2, 2025

Honorable Mayor and Members of the City Council:

This quick response audit assesses whether current offboarding guidance and procedures are sufficient to mitigate risks related to employee access to city systems and return of assigned city property upon separation of employment or transfers between departments. We found that the offboarding process is manual and decentralized across multiple agencies, and communication is inconsistent, causing network and system access to remain active beyond termination dates for some employees. The city also does not require standard documentation to track equipment issuance and return and lacks a process to ensure identification badges collected from separated employees are destroyed. Our recommendations are geared toward standardizing offboarding processes to secure assets and improving notifications to promptly revoke employee system access after termination.

The Audit Committee has reviewed this report and is releasing it in accordance with Article 2, Chapter 6 of the City Charter. We sent a draft report to management on August 28, 2025, and received responses from the responsible departments during the week of September 15, 2025. We appreciate the courtesy and cooperation of city staff throughout the audit. The team for this project was Kathy McCauley, Matthew Ervin, and Brandi Bell.

Amanda Noble
City Auditor

Donald T. Penovi, CPA
Chair, Audit Committee

Table of Contents

Audit Objectives

Processes used to offboard an employee can pose security, compliance, and operational risks. Prior audits have found instances of retired or separated employees with access to city systems or retained equipment. This audit assesses whether offboarding guidance and procedures are sufficient to mitigate these risks.

This report addresses the following objectives:

1. Are the city's current offboarding processes adequate to ensure the timely removal of employee access to city systems upon separation of employment, or when employees transfer from one city department to another?
2. How does the city ensure property has been returned upon separation of employment?

Executive Summary

What We Found

The city's offboarding process does not ensure that employee access to systems has been terminated and employee-issued equipment has been collected; as a result, the city's systems could be misused, and laptops, telephones, and Wi-Fi hotspots may not be returned when employees transfer departments or leave.

The offboarding process is manual and decentralized among multiple agencies that have critical and interdependent roles. Communication among agencies is inconsistent, causing system access to remain active beyond termination dates for some employees. In 2024, 1,830 employees left the city. We sampled 28 and found that network access for 7 employees was terminated within one day; 58% of employees sampled retained access for between 11 and 161 days beyond termination. AIM (Atlanta Information Management) tracks almost 500 systems used by the city, 34% of which have been rated as critical or of high importance to operations; however, AIM's database does not identify systems that sync to Active Directory, which allows employees to log into the city's network with one password and access multiple systems. Rehires and employees transferring to other departments also pose a risk. When employees transfer, system access should be changed to fit the employees' new role. Rehired employees may retain access to systems associated with their prior position.

The city does not require standard documentation to track equipment issuance and return, making it possible that employees have left the city and kept laptops and other issued equipment. The city also lacks a process to ensure that employee identification badges are destroyed. Former employees could access secure facilities after termination and potentially cause harm.

What We Recommended

We made nine recommendations requiring action from Human Resources, AIM, and the Mayor's Office of Emergency Preparedness. The recommendations are intended to update offboarding processes and improve notification to promptly revoke employee system access after termination. Standardizing the process should also help to ensure that city-issued equipment and identification and access badges are returned and deactivated or destroyed, better securing city systems and assets.

Background

Offboarding is the process of managing an employee's departure from an organization; it begins when the intent to separate is announced. The city's offboarding process is intended to be a collaborative effort between Human Resources, AIM, the Mayor's Office of Emergency Preparedness, and city departments to ensure that employees leaving the city experience a compliant separation process. The process includes shared responsibilities across the departments related to the return of city property, system access revocation, payroll processing, and completion of separation documentation, to ensure the continuity of operations and protection of city assets. When an employee transfers from one city department to another, best practices suggest that organizations make sure the employee does not retain access to systems that are not required for their new role.

Employee Separations or Transfers Warrant System Access Review

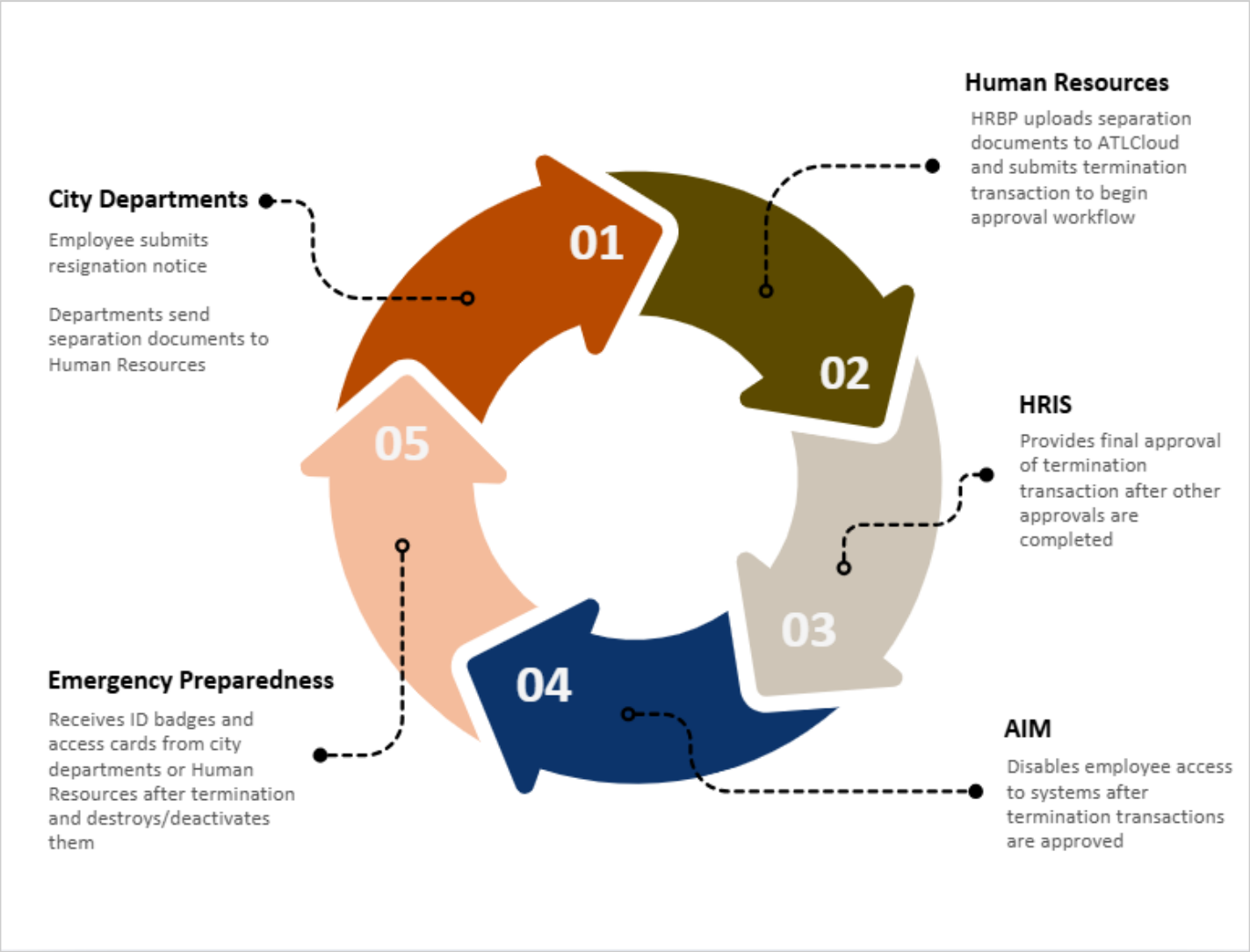
Employees leave the city either voluntarily or involuntarily. Voluntary terminations occur when an employee decides to leave willingly, generally through resignation or retirement. Involuntary terminations arise when the city initiates the dismissal of an employee, for example, in situations of misconduct, inefficient performance, or other causes. Employees may also be separated due to reductions in force, outsourcing, or death. Section 114 et seq. of city code defines the various types of employee separation.

Employees can also transfer from one department to another or to another position in the same department. Employees who leave the city in good standing could also be rehired in a prior position and department, or to a new role in another department. In either instance, system privileges should be modified to make sure that system access is aligned with an employee's current role and responsibilities.

Multiple Departments Are Responsible for the Offboarding Process

City departments, Human Resources, AIM, and the Mayor's Office of Emergency Preparedness (MOEP) play critical roles in ensuring an employee is properly separated from the city or transferred to a different department (see Exhibit 1).

Exhibit 1: Multiple Departments Are Responsible for Offboarding



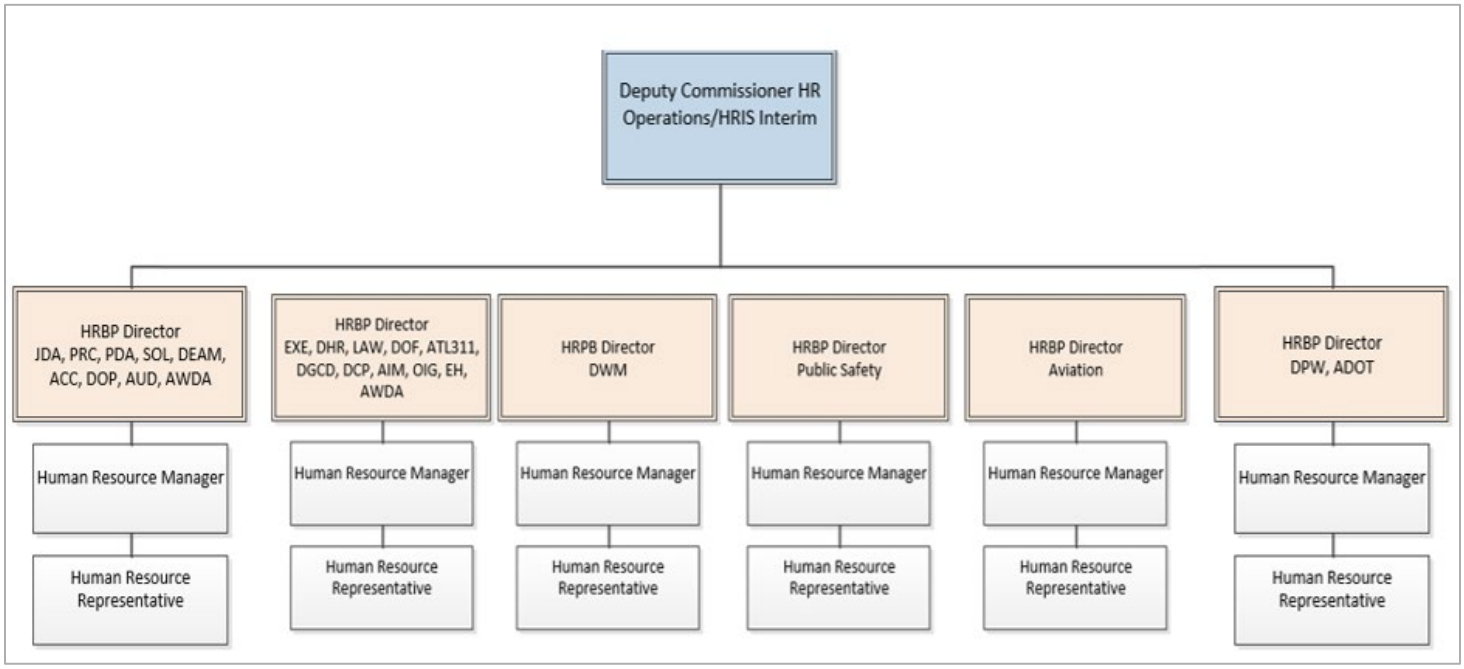
Source: Prepared by auditors from process interviews with Human Resources, AIM, and MOEP staff

- **City departments** perform specific tasks to initiate an employee offboarding from the city, depending on the separation type. When an employee resigns or retires from the city, they are expected to submit a written notice in advance of the day of resignation or retirement to their department head. Upon receipt of the notice from the employee, departments forward the resignation or retirement notice to Human Resources. For employee dismissals, department managers are required to file a copy of a document noting reasons for discharging an employee with Human Resources prior to the effective date of the dismissal.

- **Human Resources** employees, along with departments, are responsible for ensuring consistent and uniform enforcement of the city's employee

exit process. HRBPs (Human Resources Business Partners) support city departments with workforce planning tasks. HRBP teams are managed by six directors who oversee Human Resources managers and representatives, who provide support services to their assigned business units. HRBPs work with departments to make sure that termination transactions are processed, separation documents are completed, city property is collected from separated employees, and AIM staff are notified to revoke system access. The HRBP directors report to the human resources commissioner. Human Resources' HRBPs and their assigned departments are shown in Exhibit 2.

Exhibit 2: Human Resources HRBP Directors Oversee the City's Offboarding Process



Source: Auditor developed based on process interviews with Department of Human Resources staff

- **Human Resources Information System (HRIS)** employees are responsible for managing employee and position data within ATLCloud (Oracle). The HRIS team approves and finalizes employee termination transactions in ATLCloud to ensure employees have been offboarded from the system. This team also ensures separation documents are added to employees' electronic files. The HRIS team reports to a human resources deputy commissioner.

- **AIM's Office of Infrastructure and Technology** is responsible for disabling employee access to systems upon termination. AIMNow is the self-service online portal that city staff use to request assistance from AIM. City staff (either user departments or Human Resources staff) submit

service tickets to AIMNow to have system access terminated, and AIM staff receive the service requests and distribute them to the appropriate technical teams for resolution. The ATLCloud security team ensures that user accounts are disabled or assigned roles are removed from ATLCloud after an employee is terminated. AIM's server engineers disable employees' Active Directory (AD) accounts, email accounts, and most other systems that are not synced with Active Directory. They also release Microsoft licenses of separated individuals. Active Directory is a Microsoft directory service that authenticates users in a network and allows users access to multiple applications using a single set of credentials through Single Sign-On (SSO). Disabling user active directory accounts revokes or restricts access to any synced system.

AIM's telecom team is responsible for offboarding employees who were issued city mobile devices. Telecom specialists disconnect mobile device lines for terminated or transferred employees or configure the device for a new user if requested by the user department.

- **The Mayor's Office of Emergency Preparedness (MOEP)** is responsible for issuing ID badges and/or access cards to new employees when requested by the user departments. When departments or Human Resources return badges and access cards to MOEP after employees are terminated, MOEP is responsible for destroying the IDs and deactivating those access cards.

User Agencies Initiate the Termination Process After Separation

According to city code Section 114-377, when an employee resigns from the city, they must submit a written resignation letter to their department head at least 14 calendar days before their resignation date, the intended last day of work. Retiring employees notify the pension administrator of their decision to retire and provide their supervisor with 30-day advance written notice of their retirement date, which should include the employee's final date of work. The department forwards the resignation or retirement notices to Human Resources. When employees are involuntarily terminated, department managers document in writing the reasons for discharging the employee and provide the document to the terminated employee. The department also files a copy of the document with Human Resources prior to the effective date of the dismissal. A deceased employee's separation is as of the date of death.

Regardless of the separation type, departments are expected to complete the Employee Separation and Clearance Form (see Exhibit 3), which includes a checklist of tasks that should be completed to offboard an employee. Terminated employees and their supervisors are to sign the form and note whether city property has been returned, system access has been revoked, and that the employee has separated from the city without obligation. Human Resources' exit policy states that when an employee separates from the city, regardless of whether the separation is voluntary or involuntary, departments must request that AIM disable employee access immediately, effective the day of resignation or termination.

Exhibit 3: Employee Separation and Clearance Form Intended to Completely Offboard Employees

City of Atlanta

Employee Separation and Clearance Form

Submit completed form to Department of Human Resources for proper clearance. This form should be attached to the HR TAD. Failure to complete this form or to return all City properties may cause a delay in the receipt of final paycheck or cause pension benefits to be withheld.

Employee Separation Information

Name:	Employee ID No.
Department:	
Type of Separation: ☐Resigned ☐Retiring ☐Termination ☐Discharged ☐Dismissal ☐RIF/Lack of work	
Reason for Resignation or Termination:	
Date of Separation:	
Supervisor Name:	

Payout Options

Annual Leave Disbursement Options:

☐ Lump Sum Payout ☐ Leave remain payroll until exhausted ☐ No Annual Leave Due

Compensatory Time Disbursement Options:

☐ Lump Sum Payout ☐ Comp time remain on payroll until exhausted ☐ No Compensatory Time Due

Departmental Checklist

- ☐ Attach documentation to support resignation, retirement or termination to the HR TAD.
- ☐ Exit Questionnaire attached. If not, submit explanation detailing the status of exit questionnaire.
- ☐ Collect electronic equipments (PDA, cell phone, laptop or notebook pc, cameras, video or audio equipment).
- ☐ Retrieve all electronic keycards, ID badges, parking cards, or other cards allowing access to City properties.
- ☐ Collect master keys and communication devices.
- ☐ Revoke employee access and control of computers, including network logon, access to mainframe systems, Internet, Intranet and access to other databases and/or applications.
- ☐ Cancel employee access to financial or administrative MIS (Peoplesoft, Kronos, Oracle, MARS-G).
- ☐ Request Finance to review employee travel advances reimbursements, advance sick leave account, or other expensed items due to the City.
- ☐ Prepare Georgia Department of Labor Separation Notice Form DOL-800. Give original to the separated employee, mail the 2nd copy to UC eXpress, P. O. Box 283, St. Louis, MO., 63166, and file the 3rd copy in the employee's record.

Finance/Payroll Checklist/Ethics Office Notice

- ☐ Review travel advances and advance sick leave. If employee owes the City, make arrangements for restitution or make adjustments to final check, or pension.
- ☐ Cancel parking or MARTA payroll deductions.
- ☐ Secure a forwarding address for W-2 mailings.
- ☐ If the employee filed a disclosure notice over the last 12 months, the employee must file a disclosure within a year following separation.

Employee Benefits Checklist

For Retiring Employee: (These actions are done after, the department has signed the pension release form.)

- ☐ Calculate the employee's years of service to determine eligibility.
- ☐ Provide an estimate of the employee's pension benefit, as amended by Ordinance and the City Code.
- ☐ Provide medical, life, and health insurance information packet.

For Non-retiring Employee:

- ☐ Provide pension information packet, or brochure.
- ☐ Give separated employee a COBRA packet, or provide an estimate date when the packet will be available for pick-up or mailed to the forwarding address.

Final Action

☐ Pension Release Form Authorized

The separated employee has met the conditions listed on the Employee Separation and Clearance Form. All City properties have been secured, and monies due to the City of Atlanta, if any, have been recovered. The signatures below indicate that both parties, the separated employee and the supervisor/manager, agree with the contents of this form, and that the employee is separated without obligation.

_____

Separated Employee Signature and Date

_____

Supervisor or Manager Signature and Date

Source: Auditor obtained from Human Resources staff during process interview

As shown on the separation form under "payout options," separating employees with an annual leave balance may opt to take their leave as either a lump sum payment or remain on payroll until the leave is exhausted—also referred to as "riding out leave." If an employee chooses to ride out leave, the termination date will be the date that the leave is exhausted, although an employee's actual last day of work may be earlier. During this period, the employee is also accruing leave and retains health and other benefits. On September 2, 2025, City Council adopted Ordinance No. 25-O-1459 to amend city code to remove the "riding out leave" option for separating employees. Upon separation, employees entitled to annual leave with pay who terminate from the city may receive a lump sum cash payment in exchange for unused accrued annual leave.

Departments submit the form to Human Resources to add to an employee's personnel records. If an employee's signature is missing from the form, the department should document a brief statement on the employee's signature line that the employee did not sign the form.

Employee Transfers and Terminations Are Handled in ATLCloud

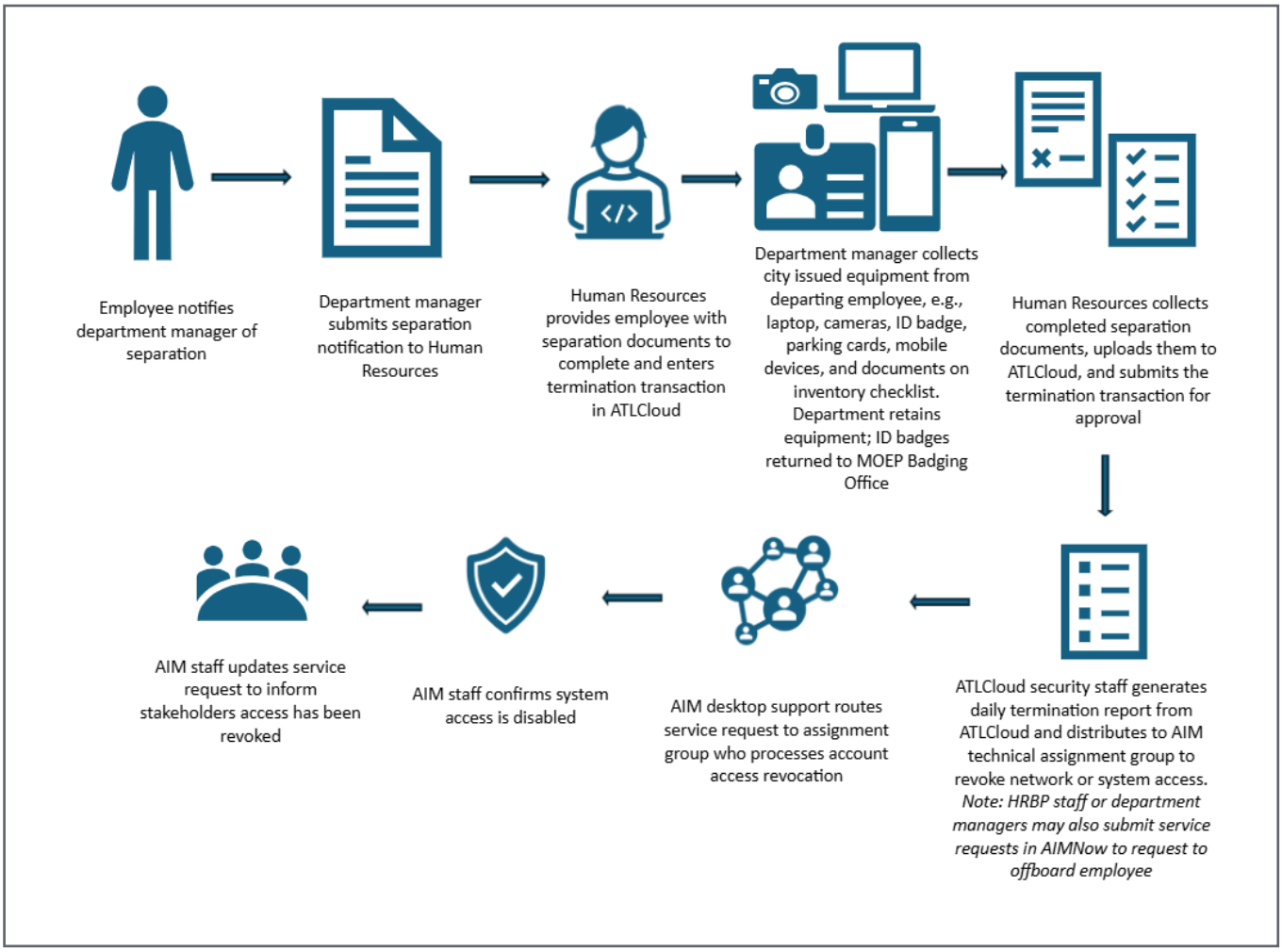
The city uses ATLCloud Human Capital Management (Oracle) to maintain employee records, including employee terminations and transfers from one department to another. All workers have an employee record created in ATLCloud when hired, and this record establishes a current, past, or future work relationship with the city. An employee's work relationship in ATLCloud provides information about their role such as job, position, compensation, managers, working hours, and location.

When a department head submits an employee's resignation letter to Human Resources, the HRBP team provides the employee with the separation documents to complete. Once HRBPs receive the resignation letters and separation forms from the user department, HRBPs initiate the offboarding transactions in ATLCloud (see Exhibit 4). The HRBP staff uploads the separation documents to the termination transaction in ATLCloud and submits the transaction for approval through the assigned workflow.

HRBP staff then enters information in ATLCloud to terminate the employee's work relationship by updating the termination effective date, specifying the termination action (i.e., "death", "involuntary termination", or "voluntary termination"), and reason for termination. When work relationships are terminated in ATLCloud, the action automatically removes a user's pre-defined roles and associated access in the ATLCloud system, but the user's account

remains active. Timely removal of system access is critical to properly offboard employees as it reduces the risk of potential data breaches. The HRBPs also notify the payroll administrator about the individual's termination so that the person's payroll can be ended. ATLCloud also allows Human Resources staff to move people between city departments as part of a transfer action, which updates the employees' record in the system.

Exhibit 4: The City's Offboarding Process Includes Manual Steps to Revoke System Access for Terminated Employees



Source: Developed by auditors based on process interviews with Human Resources and AIM staff and review of citywide offboarding policies

HRBP staff also select the scheduled time to revoke user access in ATLCloud, whether it is immediately or after the last day of work, and choose the appropriate option for rehire considerations. If an employee is separating from the city and has elected to ride out leave, Human Resources staff are required to enter the offboarding transaction as a "pre-separation" assignment in ATLCloud

to track the leave exhaustion date, which is the employee's actual termination date. Voluntary terminations require a four-step approval in ATLCloud, which includes the HRBP director, Human Resources deputy commissioner, department/division commissioner, and HRIS team member. Involuntary terminations require the same approval as voluntary terminations but must also be approved by the Human Resources commissioner before the final HRIS approval. The HRIS approval finalizes the termination transaction in ATLCloud, which triggers automatic role removal from a user's account.

AIM Deactivates Single Sign-On Access to ATLCloud

AIM staff generates a daily report from ATLCloud of finalized termination transactions that identify terminated employees whose network and system access needs to be disabled. Using this report, AIM staff deactivates the terminated employee's single-sign-on to prevent the user from logging into ATLCloud. The team also manually removes any additional roles that were not automated and audits the user's account for activity to confirm that the access has been terminated. AIM temporarily restricts access for separated employees who are riding out leave to prevent them from accessing sensitive data. If there is a predetermined leave period, the user's account is set to automatically expire at the end of the leave duration, which ensures the user's access is revoked. AIM staff notifies the appropriate stakeholders that the user's access has been revoked. AIM provides the daily termination report to other assignment groups to revoke Active Directory and other system access.

AIM maintains a database that catalogs citywide system applications. As of April 2025, the city had 497 system applications, of which 476, or nearly 96%, are documented within the database as active (see Exhibit 5). The database also captures the city department(s) that use the application, each application's criticality level, the application type, and whether the system is a public-facing application.

Exhibit 5: The City Has Nearly 500 Active System Applications

Application Status	Number of City Issued System Applications	Percentage
Active	476	96%
Pending	21	4%
Total	497	100%

Source: Auditor analysis based on review of APMS data provided by AIM Business Relationship Manager, Sr.

Staff within the assignment groups submit offboarding service requests in AIMNow that are routed by service desk agents for processing. Service requests that are routed to AIM's server or desktop teams require the engineers to disable the departing employee's Active Directory and email accounts, and to remove Microsoft licenses associated with the employee's account. When a Microsoft license is disabled, it is added back in the pool for distribution to new employees. The engineer confirms that the user's Active Directory access is disabled, and the service request is updated.

Human Resources Must Ensure City-Issued Property is Recovered

The city's employee exit process states that Human Resources staff and department managers are to ensure that all city property is recovered prior to the employee's departure. City property such as identification badges, vehicles, technology equipment, and communication devices are to be collected by the employee's department supervisor or Human Resources before the employee's final day of work. Mobile devices and other equipment collected from departing employees can be inventoried by the employee's department to be repurposed for other staff; however, mobile device transfers are to be reported to AIM to update its inventory records.

City policy states that revocation of all facility access is to occur immediately upon termination including the collection of keys, access cards, and/or any other asset used to enter restricted areas. Employees are also required to return identification badges to Human Resources staff as part of the exit interview, who are to provide them to the Mayor's Office of Emergency Preparedness for further processing. When an employee transfers from one city department to another, the department supervisor to whom the employee reported prior to the transfer is responsible for ensuring system access is revoked and city property belonging to the employee's former department is recovered.

1,830 Employees Left the City Between January and December 2024

From January 1, 2024, through December 31, 2024, the city had 1,837 separation transaction actions in ATLCloud for 1,830 employees. There were more transactions than employees because seven employees were rehired after leaving and were terminated a second time within the same year. The Departments of Parks and Recreation, Aviation, and Police account for 56% of the terminations processed during this time period (see Exhibit 6).

Exhibit 6: Nearly 56% of Employee Terminations Were From 3 Departments

Department Name	Number of Termination Actions	Percentage
Parks and Recreation	559	30.4%
Aviation	248	13.5%
Police	221	12.0%
Public Works	140	7.6%
Watershed Management	135	7.3%
Fire	101	5.5%
Executive Offices	61	3.3%
Corrections	55	3.0%
City Planning	46	2.5%
Finance	34	1.9%
Customer Service	32	1.7%
City Council	31	1.7%
AIM	27	1.5%
Human Resources	25	1.4%
ATLDOT	24	1.3%
Judicial Agencies	24	1.3%
Law	21	1.1%
Procurement	12	0.7%
Grants	9	0.5%
Solicitor's Office	8	0.4%
Labor & Employment	8	0.4%
DEAM	4	0.2%
Public Defender	4	0.2%
Audit	4	0.2%
ACRB	3	0.2%
Ethics	1	0.1%
Total	1,837	100%

56%

Source: Auditor analysis of ATLCloud data as of May 22, 2025; represents terminations from these departments between January 1, 2024, through December 31, 2024

Of the 1,837 separation transactions processed during the period, slightly over 40% were employees categorized in the civil service system as classified (see Exhibit 7). Unclassified service personnel are employees in salary grades 19 and above and can consist of elected officials, mayoral appointments, sworn employees in public safety departments such as Police and Fire, and judicial agency employees. Classified employees include employees in salary grades below 19. Higher-level employees can pose greater risks if not properly offboarded because they tend to have access to more sensitive data and greater access rights.

Exhibit 7: Slightly Over 40% of Terminations Processed Were for Classified Employees

Grade Category	Number of Termination Actions	Percentage
Grade 18 and Below	745	41%
Seasonal	498	27%
Grade 19 and Above	359	20%
Police	147	8%
Fire	53	3%
Corrections	21	1%
Council	9	0%
Executive	5	0%
Total	1,837	100.0%

Source: Auditor analysis of ATLCloud data as of May 22, 2025; represents terminations from these departments between January 1, 2024, through December 31, 2024

At Least 134 Employees Transferred Between Departments in CY24

From January 1, 2024, through December 31, 2024, the city had 179 transfer actions for 134 employees for the period. Interdepartmental transfers to Watershed accounted for nearly 24% of the transfers identified during the period (see Exhibit 8).

Exhibit 8: The City Had Nearly 200 Interdepartmental Transfers During CY 2024

Destination Department Name	Number of Transfer Actions	Percentage
Watershed Management	42	24%
ATLDOT	26	15%
Executive Offices	17	10%
Aviation	16	9%
Police	10	6%
Human Resources	10	6%
Labor & Employment	9	5%
Public Works	7	4%
City Planning	6	3%
Finance	6	3%
Fire	4	2%
City Council	4	2%
Grants	4	2%
Parks and Recreation	3	2%
Corrections	3	2%
AIM	3	2%
Procurement	3	2%
Customer Service	2	1%
DEAM	2	1%
Law	1	1%
Solicitor's Office	1	1%
Total	179	100%

Source: Auditor analysis of ATLCloud data as of June 5, 2025; represents transfers to these departments from January 1, 2024, through December 31, 2024

It should be noted that the transfer actions identified in our analysis may not be all interdepartmental transfers for the period; some employees may have been transferred between departments without processing a transfer action in ATLCloud. These numbers may also be slightly off in aggregate if employees changed departments but also had an intradepartmental transfer action within the same period or if there were any employees processed improperly in ATLCloud.

Nearly 50% of the interdepartmental transfers for the period were employees in grades 19 and above who are categorized as unclassified service personnel (see Exhibit 9).

Exhibit 9: The Majority of Interdepartmental Transfers for 2024 Were for Employees with Salary Grades of 19 and Above

Grade Category	Number of Transfers	Percentage
Grade 19 and Above	86	48%
Grade 18 and Below	84	47%
Blank	5	3%
Council	2	1%
Executive	1	1%
Seasonal	1	1%
Total	179	100%

Source: Auditor analysis of ATLCloud data as of June 5, 2025; represents transfers from these departments between January 1, 2024, through December 31, 2024

Findings and Analyses

Objective 1: Are the city's current offboarding processes adequate to ensure the timely removal of employee access to city systems upon separation of employment, or when employees transfer from one city department to another?

The city's process to revoke system and network access for offboarded employees is decentralized and manual, although best practices recommend that the process be automated. Requests to terminate employees must be submitted as transactions in ATLCloud (Oracle) to separate employees and discontinue payroll. The request must be approved by several employees before being finalized and sent to AIM to terminate system access. Termination of system access for separated employees can also be requested directly through a service ticket to AIM, initiated by user departments or Human Resources staff. The ATLCloud termination request must be approved by the HRBP director, department commissioner, Human Resources deputy commissioner and/or commissioner, and an HRIS team member, depending on the type of termination action. This process could take weeks, and once the transaction is approved, AIM staff must pull a report from ATLCloud to identify terminated employees who need system access revoked. Service requests to AIM to discontinue system access could be processed faster, but manually disabling access can be time-consuming and prone to errors, leading to delays and security vulnerabilities.

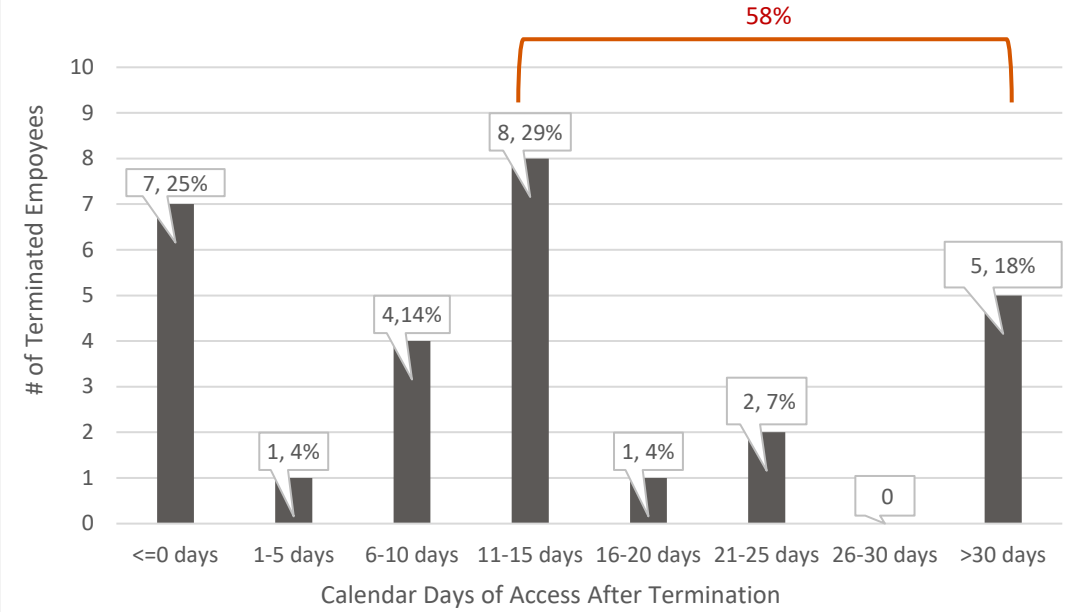
Offboarding is Manual, Leading to Continued System Access After Termination

We reviewed network and system access of terminated and transferred city employees and found that some employees retained system access beyond their termination date, or after they transferred to other departments. Employee access should be revoked as soon as possible upon termination, according to best practices, to ensure city systems and assets are secure. Employees may have access to systems that they should not have access to, including transactional access, with which "bad actors" could cause harm.

21 of 28 Sampled Employees Retained Network Access After Termination

We found that the city typically takes longer than recommended to disable network accounts for terminated employees. Of our sample of 28 employees terminated in 2024, we found that system access for 7 employees was terminated within 1 day, consistent with best practices. Of the 28, we identified 21 who retained access for between 3 and 161 days, with a median number of days of access after termination of 15 days. Failure to promptly disable network accounts for terminated employees creates significant security risks, such as potential misuse of access to systems and sensitive data by former employees. Exhibit 10 shows the number of employees who retained system access beyond their termination dates, measuring the number of calendar days from the employee's effective termination date to the network (Active Directory) access termination date.

Exhibit 10: We Identified 21 Employees Who Retained System Access Between 3-161 Days After Termination Date



Source Developed by auditors based on sample test results of network (Active Directory) access revocation for employees terminated in 2024, pulled from ATLCloud (Oracle) Transactional Business Intelligence (OTBI) report generated as of May 22, 2025, and representing terminations during CY24

Best practices suggest that access to systems should be removed by the next business day following termination to prevent unauthorized access; however,

disabling access immediately upon termination or automating access disablement can prevent potential data issues or misuse.

Our sample was selected as follows: in calendar year 2024, the city had 1,837 separation transactions for 1,830 employees. In our testing, we excluded 1,473 termination transactions for specific groups of employees, including those categorized as council, public safety, and seasonal staff, leaving a population of 364 termination transactions for sampling. We selected a sample of 38 terminated employees—5 employees at executive salary grades and a stratified sample of 33 employees with grades 19 and above, as these employees inherit more risk than those with lower salary grades due to the level of access that could be assigned to their roles. We were unable to locate service tickets in AIMNow for 10 terminated employees to determine whether network access has been deactivated, therefore, our remaining sample included 28 employees. For those employees, we analyzed the number of calendar days from the employee's effective termination date to the actual access termination date.

System User Accounts Remain Active for Terminated and Transferred Employees

We tested four city systems to assess whether active user accounts were disabled timely upon employee termination or transfer: Accela, enQuesta, Airport Business Revenue Management (ABRM), and EnerGov, which different city departments use to process financial and permitting transactions (see Exhibit 11). These systems were rated by the city as being of critical, high, or medium importance to operations.

We reviewed access to these systems and found multiple active user accounts in Accela and enQuesta of employees who were terminated from the city, dating back to 2014. Additionally, we identified an employee who was terminated in 2022 from one department that uses enQuesta and rehired in 2023 by the city in another department that does not use the system, but the employee still has an active account in enQuesta. We did not identify active accounts for users terminated from the city in the EnerGov and ABRM systems.

Although an active user account exists, it doesn't mean that an employee has accessed the system. We conducted testing in Accela and enQuesta to identify any login activity on the active user accounts and did not find any activity. We did not test each system to identify whether the employees have certain access or system privileges with the active accounts.

We identified examples of employees who transferred to other city departments but have active system accounts that are no longer needed. Two employees with active accounts in EnerGov transferred to other positions but continued to have active user accounts in the system. For example, one employee who had an active account in EnerGov transferred in March 2025 from one business unit that uses the system to another unit within the same department that does not use EnerGov. However, we found the employee still had an active system account that the system administrator deactivated in July 2025 upon our inquiry.

Another user had an active system account in EnerGov that we found to be a contingent worker; however, the system administrator told us the user is no longer with the assigned business unit and deactivated the account upon our inquiry.

We also identified employees who transferred from the Watershed Department in 2022 to another department but still have active enQuesta accounts. Best practices suggest that organizations review and confirm ongoing operational needs for current logical access authorizations to systems when individuals are reassigned or transferred to other positions in the organization. Access should be modified as needed to correspond with any changes in operational need due to reassignment or transfer.

Exhibit 11: We Tested Four City Systems with Criticality Rankings from Critical to Medium

System Application	City Departments That Use the System Application	System Application Purpose	Criticality Level
Accela	Fire, Planning, Police, Transportation, and Watershed Management	Cloud based platform various city departments use for permitting, code inspections and violations, and review of site plans and zoning requests.	Critical
EnQuesta	Watershed Management	Customer information system Watershed Management uses for processing water billing activities.	Critical
EnerGov	ATL311, Finance, and Police	System various city departments use for issuing business licenses and alcohol permits, managing occupational tax certificates, and handling customer service requests.	High
Airport Business Revenue Management (ABRM)	Aviation	Financial software Aviation uses for utilities billing, invoicing, and accounts receivable.	Medium

Source: Developed by auditors based on APMS Database as of 4/29/2025, Atlanta Information Management

Users with a Pre-Separation Status in ATLCloud Should Have Restricted Access

Employees who have separated from the city, but elected to "ride out leave," meaning they have terminated but are on payroll until their annual leave is exhausted, have user profiles in ATLCloud in pre-separation status. System access is restricted for these users to make sure they do not have system roles and privileges that allow them access to sensitive data and functions, but they can still access basic information, such as payroll or benefits information.

We identified five employees who have pre-separation status in ATLCloud as of June 24, 2025. Of these five, two users still had transactional (non-inquiry) roles in ATLCloud. One user was in a project manager position as of March 2025 and had hiring manager and receipting roles assigned to their profile. The other user was in a policy director position as of June 2025 and still has hiring manager and manager self-service roles in ATLCloud. Users with hiring manager roles can hire candidates and those with receipting roles can prepare requisitions and have access to advanced requisition creation permissions in the system. The manager self-service role can have customized managerial system permissions in ATLCloud.

Without timely disablement of network or system access, terminated or transferred employees may still have access to sensitive information or log into accounts, which could potentially cause harm. **We recommend the human resources commissioner add a notification earlier in the termination transaction workflow to notify appropriate AIM staff that a user has terminated from the city, or that a pre-separation status was entered for the user to ensure that system and network access is revoked more timely**.

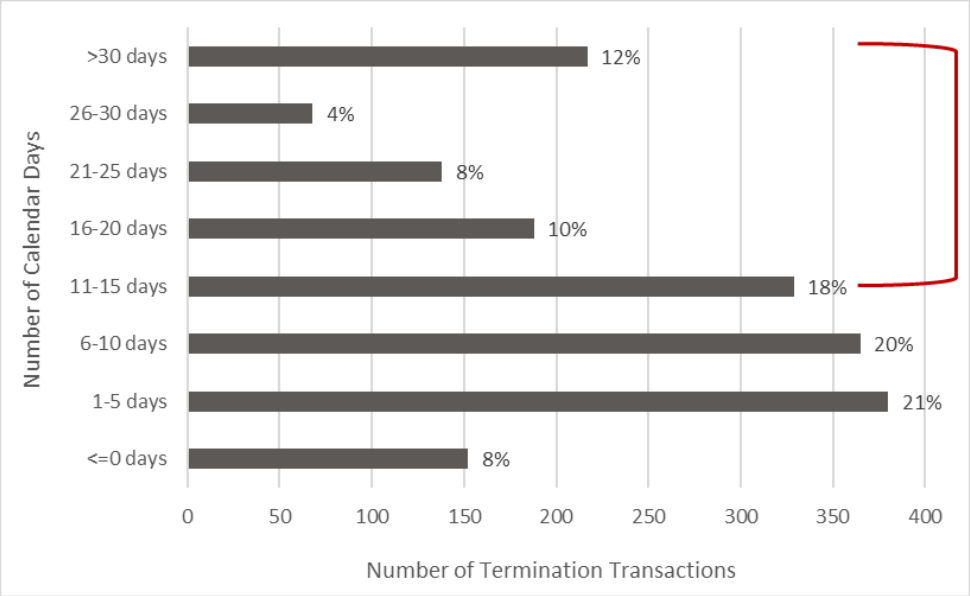
Human Resources Lacks Service Level Agreements that Address Employee Offboarding Activities

Current Human Resources service level agreements (SLAs) do not include turnaround times to offboard employees and process termination transactions. Best practices state that while each termination may be unique, planning for each termination type should include delegation of tasks and timelines for the completion of each task.

Over Half of Termination Transactions Took Longer Than Ten Days to Process

When we reviewed termination transactions occurring during calendar year 2024, we found that over half took longer than ten days to complete (see Exhibit 12). Once the termination transactions are approved by human resources staff, AIM staff can pull a report from ATLCloud indicating employees who have been terminated and need their system access revoked. To ensure that employee system access is revoked more timely, Human Resources should notify AIM of an employee's impending departure at least five business days prior to the last day of employment.

Exhibit 12: 51% of Employee Termination Transactions Processed in CY 2024 Took Longer Than Ten Days to Complete



Source: Developed by auditor from Terminations Report data (Termination transactions from January through December 2024) pulled from ATLCloud (Oracle) Transactional Business Intelligence

Delayed approval of termination transactions in ATLCloud prolongs notification to AIM to remove terminated employee's network and system access since it is a manual process and relies on communication from Human Resources or user departments. **We recommend the human resources commissioner develop SLAs for the HRBPs to enter offboarding transactions in ATLCloud and for HRIS staff to approve the transactions.** This should help to ensure offboarding transactions are processed sooner.

AIM Does Not Maintain a Listing of Citywide System Applications that Are Synced with Active Directory

AIM uses a database to catalog nearly 500 citywide system applications. The city has rated 34% of these applications as critical or of high importance to its

operations, meaning the city needs the system application to operationally function or sudden system downtime could result in a significant impact to city services. Although AIM disables employee access to Active Directory accounts, some terminated employees may also have access to other city systems that are not synced with Active Directory. This access may need to be revoked separately either by AIM staff or user departments who own those systems.

Lack of Awareness of System Applications Synced with Active Directory Creates Access and Security Risks

We requested from AIM a listing of citywide applications that are synced with Active Directory, since it allows employees to log into the city's network with one password and access multiple systems. AIM told us the department was unable to provide a listing of the systems used across the city that sync to Active Directory. This could lead to terminated or transferred employees having unnecessary system access or active accounts of which system administrators may be unaware. AIM currently maintains a repository of systems used throughout the city. After our audit fieldwork concluded, AIM provided a listing of systems that are single sign-on enabled. It would be beneficial to document system applications synced or not synced with Active Directory to ensure security, compliance, and operational risks are mitigated and system access is effectively managed. AIM told us they are working with Human Resources to automate the offboarding process, including identifying systems to which employees were given access when they were onboarded with the city. However, AIM does not manage all systems used across the city, which suggests a process is needed to inform system administrators when an employee leaves the city to ensure all assigned systems, including the systems that are not under AIM's purview, are disabled upon termination. **We recommend that the chief information officer indicates in the department's current citywide system repository whether each system is synced with Active Directory**. **We also recommend that the chief information officer work with the human resources commissioner to ensure a process is put in place to notify the appropriate system administrators of critical applications requiring deactivation.**

Objective 2: How does the city ensure property has been returned upon separation of employment?

The city's process to document collected equipment from terminated employees is inconsistent among departments. There is also no process in place to reconcile assigned property to returned property upon employee termination.

The City Doesn't Consistently Track Equipment Issuance and Return

Human Resources policy states that when an employee separates from the city, the employee is expected to return assigned city equipment to the issuing department, which is responsible for conducting an inventory to confirm that all assigned equipment has been returned and to verify the condition of returned equipment for damage purposes. We found the city does not maintain documentation that all issued equipment was returned.

The City Lacks a Process to Ensure the Return of Assigned Property from Terminated Employees

Departments are to collect city property such as electronic equipment, mobile devices, identification badges, keys, parking cards, and other cards allowing access to city property, by the employee's resignation or termination date. User department managers document the collection of property on the Employee Separation and Clearance Form (see Exhibit 3), then provide the form to Human Resources to upload to the termination transaction in ATLCloud either on or before an employee's last day of work. The form must be signed by the separating employee and manager as the signatures indicate that both parties agree with the contents of the form and that the employee has separated without obligation. The Employee Separation and Clearance Form does not reconcile collected city property to property that was assigned to the separating employee. User departments can also use an internal checklist to document returned property. The city does not have a standardized checklist in place to ensure the process is consistent citywide for the return of assigned city property from separating employees.

We reviewed termination transactions across different departments to identify whether assigned city property was collected from separated employees upon termination. It was not possible to confirm that city property was consistently returned from terminated employees because departments are not typically documenting assigned equipment; making it difficult to reconcile returned or collected city property. We also found that the separation documentation for separated employees which should note the collection of city property was either incomplete, unsigned, or not present. **We recommend the human resources commissioner develop a standardized checklist to be used citywide by departments to note both issuance and collection of city property and disseminate the checklist along with the updated Employee Exit Process policy. We also recommend the human resources commissioner ensure separation documents are complete and signed before being uploaded to ATLCloud.**

We further recommend the human resources commissioner include verbiage in the updated Employee Exit Process policy regarding the recovery of property if it is not returned within a defined timeframe, ensuring that the policy explicitly states that the failure to return city equipment is considered as theft.

Terminated Employee Identification Badges and Access Cards Are Not Properly Collected or Disposed

Responsibilities for disposal of identification badges and access cards from terminated employees are not clearly documented once they are collected by Human Resources or departments. Human Resources staff told us that when identification badges and access cards are collected, they may be returned to MOEP (Mayor's Office of Emergency Preparedness) for deactivation, except for departments that handle their own ID badge security—such as Watershed Management, Corrections, Police, Fire, and Aviation. However, we found that MOEP is not notified when employees have been terminated, making it difficult to ensure that ID badges and access cards are deactivated. This creates potential security risks as former employees could gain unauthorized access to secured facilities after termination using IDs and badges.

City Has No Process for ID Badge & Access Card Collection and Disposal

MOEP is responsible for issuing identification badges and access cards to some city employees and contractors. This responsibility was previously under the

purview of Enterprise Assets Management but was moved to MOEP in 2022. The badge includes the individual's name, photo, and department and in some cases can be used as an electronic key to enter city buildings and other secured areas as needed. We identified during interviews with MOEP staff that its badging office collects identification badges and access cards of terminated employees; however, a process does not exist to ensure employee ID badges and access cards from terminated employees are destroyed upon collection. For example, MOEP staff explained that departments sometimes randomly leave identification badges and access cards on the front desk in MOEP's office with no explanation

Title: MOEP staff found a bag of ID badges left on desk with no documentation.
Source: Photo taken by auditors during walkthrough with MOEP security team on 5/26/2025

Title: ID badges and access cards collected from terminated employees are stored in a box behind the security specialist's desk.
Source: Photo taken by auditors during observation with MOEP security team on 5/26/2025

(see photo). Staff told us that the office is not notified when employees are terminated, requiring MOEP to collect and deactivate ID badges and access cards. Staff from AIM also told us that the MOEP team is not part of the distribution list that receives the daily termination report, which includes information about employees who have terminated from the city.

When identification badges with entry access are collected from offboarded employees, MOEP deactivates the employees' access in the access security system; however, the collected badges are not destroyed; they are stored in boxes behind a desk in the badging office (see photo). MOEP staff told us that collected ID badges and access cards were also stored in boxes in an unlocked area in city hall. We tried to view these, but MOEP's security team could not locate them. We only found one contractor badge that was left on the floor (see photo). MOEP staff told us they don't log the badges for tracking purposes when they are collected from terminated employees.

Title: Contractor badge left on the floor where staff told us ID badges were stored.
Source: Photo taken by auditor during an observation conducted with the MOEP security team on 5/26/2025

Best practices suggest that identification and access badges collected at employee termination should be properly disposed, including shredded, to ensure that access to the business and its sensitive information is controlled. **We recommend the Human Resources commissioner update the Employee Exit Process policy to ensure guidance is provided to city departments regarding the return of identification badges from terminated employees to Emergency Preparedness.** We also recommend that the chief information officer ensure the daily terminations distribution list includes the MOEP security team so that MOEP can collect and deactivate identification badges and access cards of terminated employees. AIM staff told us they implemented this recommendation after we brought it to their attention, and we confirmed that it was implemented.

We further recommend the emergency preparedness executive director collaborate with the human resources commissioner to execute a policy for the logging, tracking, and disposal of identification badges collected from separating employees.

Recommendations

To align city processes for the revocation of system access for terminated or transferred employees with best practices, the human resources commissioner should:

1. add a notification earlier in the termination transaction workflow to notify appropriate AIM staff that a user has terminated from the city or a pre-separation status was entered for the user to ensure that system and network access is revoked more timely

To ensure user departments and Human Resources staff have a clear understanding of related offboarding responsibilities and termination transactions are processed timely, the human resources commissioner should:

2. develop SLAs for the HRBPs to enter offboarding transactions in ATLCloud and for HRIS staff to approve the transaction to ensure offboarding transactions are processed consistently and to keep client groups informed on service level expectations and response times for performing various offboarding tasks

To improve the tracking of collected property and equipment from separated employees, the human resources commissioner should:

3. ensure separation documents are complete that note the return of city property from terminated employees, including signatures acknowledging the receipt of equipment before being uploaded to ATLCloud
4. develop a standardized checklist to be used citywide by departments to note the collection of city property and disseminate the checklist along with the updated Employee Exit Process policy; the checklist should reconcile assigned property to returned property to ensure all city equipment has been collected
5. include verbiage in the updated Employee Exit Process policy regarding the recovery of property if it is not returned within a defined timeframe, ensuring that the policy explicitly states that the failure to return city equipment is considered as theft
6. update the Employee Exit Process policy to ensure guidance is provided to city departments regarding the return of identification badges from terminated employees to Emergency Preparedness

To effectively manage system access and ensure security risks are addressed, the chief information officer should:

7. indicate in the department's current citywide system repository whether each system is synced with Active Directory
8. work with the human resources commissioner to ensure a process is put in place to notify the appropriate system administrators of critical applications requiring deactivation

To prevent terminated employees from accessing city facilities they no longer have authorized access to, the emergency preparedness executive director should:

9. collaborate with the human resources commissioner to execute a policy for the logging, tracking, and disposal of identification badges collected from separating employees

Appendix A: Management's Response

Report Title: Offboarding	**Project No.** 25.06

Recommendation #1:
We recommend that the human resources commissioner add a notification earlier in the termination transaction workflow to notify appropriate AIM staff that a user has terminated from the city, or that a pre-separation status was entered for the user to ensure that system and network access is revoked more timely.

Risk Category:	**Recommendation Priority:**	**Auditee Response:**
Information Security	Medium	Agree

Related Finding(s):

- We reviewed network and system access of terminated and transferred city employees and found that some employees retained system access beyond their termination date, or after they transferred to other departments.
    - Of our sample of 28 employees terminated in 2024, we found that system access for 7 employees was terminated within 1 day, consistent with best practices. Of the 28, we identified 21 who retained access for between 3 and 161 days, with a median number of days of access after termination of 15 days.
    - We tested four city systems to assess whether active user accounts were disabled timely upon employee termination or transfer and found multiple active user accounts of employees who were terminated from the city, dating back to 2014. We also identified employees who transferred between city departments that continued to have active user system accounts that are no longer needed.
    - We identified five employees who have pre-separation status in ATLCloud as of June 24, 2025. Of these five, two users still had transactional (non-inquiry) roles in ATLCloud. One user was in a project manager position as of March 2025 and had hiring manager and receipting roles assigned to their profile. The other user was in a policy director position as of June 2025 and still has hiring manager and manager self-service roles in ATLCloud.

Proposed Action:
HRIS and Deloitte started a Onboarding/Offboarding project since June 2025 to utilize the Journeys module for Terminations. For context, Journeys is currently being used for Onboarding. We are exploring utilizing an integration between ATLCloud and ServiceNow to streamline the process for auto-generation of AIM tickets. This will act as the automated notification to disable user accounts based on the termination date for the AIM department.

Name & Title of Business Owner:	**Current Status:**	**Estimated Implementation Date Month/Year):**
Cedric Stimphil, Director of HRIS	Started	10/2025

Recommendation #2:
We recommend that the human resources commissioner develop SLAs for the HRBPs to enter offboarding transactions in ATLCloud and for HRIS staff to approve the transactions.

Risk Category:	**Recommendation Priority:**	**Auditee Response:**
Information Security	Medium	Agree

Related Finding(s):

- We reviewed termination transactions occurring during calendar year 2024, and we found that over half took longer than ten days to complete.
    - Delayed approval of termination transactions in ATLCloud prolongs notification to AIM to remove terminated employee's network and system access since it is a manual process and relies on communication from Human Resources or user departments.

Proposed Action:
The Department of Human Resources will incorporate the following language, or substantially similar, into the Citywide Employee Exit Process policy:
"The HR team must enter all separation transactions no later than one business day after an employee's final day of employment with the City. HR and departmental staff must review and approve separation transactions within one business day of receipt."

Name & Title of Business Owner:	**Current Status:**	**Estimated Implementation Date Month/Year):**
Tenill Ransom, HRBP Director	Started	December 1, 2025, or upon review, approval by the appropriate parties, and publication for Citywide use.

Recommendation #3:
We recommend that the human resources commissioner ensure separation documents are complete and signed before being uploaded to ATLCloud.

Risk Category:	**Recommendation Priority:**	**Auditee Response:**
Asset Misappropriation	Low	Agree

Related Finding(s):

- We found that the separation documentation for separated employees which should note the collection of city property was either incomplete, unsigned, or not present.
    - We reviewed termination transactions across different departments to identify whether assigned city property was collected from separated employees upon termination. Since departments are not typically documenting assigned equipment, it was not possible to confirm that city property was consistently returned from terminated employees.

Proposed Action:
DHR will add verbiage to the draft Employee Exit Process policy that requires HR teams to ensure that all separation documents are complete and signed before being uploaded to ATLCloud.

Name & Title of Business Owner:	**Current Status:**	**Estimated Implementation Date Month/Year):**
Tenill Ransom, HRBP Director	Started	December 1, 2025, or upon review, approval by the appropriate parties, and publication for Citywide use.

Recommendation #4:
We recommend that the human resources commissioner develop a standardized checklist to be used citywide by departments to note both issuance and collection of city property and disseminate the checklist along with the updated Employee Exit Process policy.

Risk Category:	**Recommendation Priority:**	**Auditee Response:**
Asset Misappropriation	Low	Agree

Related Finding(s):

- User department managers document the collection of property on the Employee Separation and Clearance Form, then provide the form to Human Resources to upload to the termination transaction in ATLCloud either on or before an employee's last day of work.
    - The Employee Separation and Clearance Form does not reconcile collected city property to property that was assigned to the separating employee. User departments can also use an internal checklist to document returned property, which indicates the city does not have a standardized checklist in place to ensure the process is consistent citywide for the return of assigned city property from separating employees.

Proposed Action:

DHR has drafted revisions to the Citywide Employee Exit Process policy to include an HR Inventory Return Checklist. The policy is pending review and approval by the appropriate parties. Once approved, the checklist will serve as a standardized form for all departments to document the issuance and collection of City property and will be published on the intranet along with policy documents.

Name & Title of Business Owner:	**Current Status:**	**Estimated Implementation Date Month/Year):**
Tenill Ransom, HRBP Director	Started	December 1, 2025, or upon review, approval by the appropriate parties, and publication for Citywide use.

Recommendation #5: We recommend that the human resources commissioner include verbiage in the updated Employee Exit Process policy regarding the recovery of property if it is not returned within a defined timeframe, ensuring that the policy explicitly states that the failure to return city equipment is considered as theft.		
Risk Category: Asset Misappropriation	**Recommendation Priority:** Low	**Auditee Response:** Agree
Related Finding(s): • We reviewed termination transactions across different departments to identify whether assigned city property was collected from separated employees upon termination. It was not possible to confirm that city property was consistently returned from terminated employees because departments are not typically documenting assigned equipment; making it difficult to reconcile returned or collected city property.		
Proposed Action: **DHR will include the following verbiage, or substantially similar, in the draft Employee Exit Process Policy:** *"Any separating employee who fails or refuses to return City property upon separation may be considered to have committed an act of theft. In such cases, the City reserves the right to pursue any and all remedies available under applicable laws."*		
Name & Title of Business Owner: Tenill Ransom, HRBP Director	**Current Status:** Started	**Estimated Implementation Date Month/Year):** December 1, 2025, or upon review, approval by the appropriate parties, and publication for Citywide use.

Recommendation #6: We recommend that the human resources commissioner update the Employee Exit Process policy to ensure guidance is provided to city departments regarding the return of identification badges from terminated employees to Emergency Preparedness.		
Risk Category: Public Safety	**Recommendation Priority:** High	**Auditee Response:** Agree
Related Finding(s): • Responsibilities for disposal of identification badges and access cards from terminated employees are not clearly documented once they are collected by Human Resources or departments. Human Resources staff told us that when identification badges and access cards are collected, they may be returned to MOEP (Mayor's Office of Emergency Preparedness) for deactivation. However, we found that MOEP is not notified when employees have been terminated, making it difficult to ensure that ID badges and access cards are deactivated.		
Proposed Action: **MOEP does not issue badges for all City departments. Certain offices, such as DWM and Aviation, issue their own badges, which must be returned directly to the applicable office. To address this recommendation, DHR will add the following language, or substantially similar, to the draft Employee Exit Process policy:** *"Departments are responsible for ensuring that all City property collected from separating employees, including equipment, identification badges, vehicles, technology, communication devices, and other assets, is returned to the issuing department or office for proper deactivation and completion of termination processes."*		
Name & Title of Business Owner: Tenill Ransom, HRBP Director	**Current Status:** Started	**Estimated Implementation Date Month/Year):** December 1, 2025, or upon review, approval by the appropriate parties, and publication for Citywide use.

Recommendation #7: We recommend that the chief information officer indicates in the department's current citywide system repository whether each system is synced with Active Directory.		
Risk Category: Information Security	**Recommendation Priority:** Medium	**Auditee Response:** Agree
Related Finding(s): • We requested from AIM a listing of citywide applications that are synced with Active Directory, since it allows employees to log into the city's network with one password and access multiple systems. AIM initially told us the department is unable to provide a listing of the systems used across the city that sync to Active Directory. This could lead to terminated or transferred employees having unnecessary system access or active accounts of which system administrators may be unaware. AIM currently maintains a repository of systems used throughout the city. After our audit fieldwork concluded, AIM leadership provided a listing of systems that are single sign-on enabled. It would be beneficial to document system applications synced or not synced with Active Directory to ensure security, compliance, and operational risks are mitigated and system access is effectively managed.		
Proposed Action: The application repository used by AIM will be updated to include a column that indicates whether or not the system is single sign-on (SSO) enabled.		
Name & Title of Business Owner: Kentorri Garmon	**Current Status:** Not Started	**Estimated Implementation Date Month/Year):** December, 2025

Recommendation #8: We recommend that the chief information officer work with the human resources commissioner to ensure a process is put in place to notify the appropriate system administrators of critical applications requiring deactivation.		
Risk Category: Information Security	**Recommendation Priority:** Medium	**Auditee Response:** Agree
Related Finding(s): • AIM told us they are working with Human Resources to automate the offboarding process, including identifying systems to which employees were given access when they were onboarded with the city. However, AIM does not manage all systems used across the city, which suggests a process is needed to inform system administrators of when an employee leaves the city to ensure all assigned systems, including the systems that are not under AIM's purview, are disabled upon termination.		
Proposed Action: This requirement will be added to the offboarding project, which is currently active.		
Name & Title of Business Owner: Kentorri Garmon	**Current Status:** Not Started	**Estimated Implementation Date Month/Year):** To be confirmed by project team.

Recommendation #9:
We recommend that the emergency preparedness executive director collaborate with the human resources commissioner to execute a policy for the logging, tracking, and disposal of identification badges collected from separating employees.

Risk Category:	**Recommendation Priority:**	**Auditee Response:**
Public Safety	Medium	Agree

Related Finding(s):

- We identified during interviews with MOEP staff that its badging office collects identification badges and access cards of terminated employees; however, a process does not exist to ensure employee ID badges and access cards from terminated employees are destroyed upon collection.
    - When identification badges with entry access are collected from offboarded employees, MOEP deactivates the employees' access in the access security system; however, the collected badges are not destroyed; they are stored in boxes behind a desk in the badging office or in boxes in an unlocked area in city hall. MOEP staff told us they don't log the badges for tracking purposes when they are collected from terminated employees.

Proposed Action: The MOEP Team will do the following:

Badge Logging & Secure Storage: MOEP has implemented a process to log all returned identification badges and temporarily secure them in a locked room until certified destruction occurs.

Policy Integration with HR: MOEP will collaborate with Human Resources to finalize a comprehensive ID Badge Policy aligned with their broader offboarding procedures.

Technology Integration (HR & AIM): MOEP, HR, and AIM will coordinate on an integrated technology solution that connects ID badging and access control applications with HR systems to ensure seamless tracking, deactivation, and compliance.

Name & Title of Business Owner:	**Current Status:**	**Estimated Implementation Date Month/Year):**
Andre Kearns	Partly Implemented	To be confirmed with the various collabrating teams

Appendix B: Scope and Methodology

We conducted this audit in accordance with generally accepted government auditing standards. Our audit included a review of employee termination and departmental transfer transactions generated from ATLCloud for the period of January 1, 2024, through December 31, 2024. Our testing excluded termination and transfer transactions related to seasonal employees, employees with civil service grades of 18 and below, public safety employees, and council staff. Our audit included a review of the city's overall offboarding process; it does not include a focus on internal offboarding processes of user departments.

Our audit methods included:

- reviewing city code provisions to understand employee offboarding requirements
- reviewing Human Resources and AIM policies and procedures to identify guidance provided to departments to properly separate employees from the city or reassign them to other departments
- reviewing best practices for revoking system access and recovering property upon an employee's departure
- interviewing Human Resources, AIM, and Emergency Preparedness staff to understand current offboarding practices
- analyzing termination transactions processed in ATLCloud during our scope to determine the average number of days taken to finalize terminations beyond an employee's termination date
- performing reviews of exit clearance forms to determine if they appropriately track whether terminated employees return assigned city property upon their departure
- analyzing the median number of days network access was enabled for sampled terminated employees beyond their termination date
- evaluating whether terminated and transferred employees in our scope maintained active system accounts beyond their termination date
- identifying whether processes exist to ensure identification badges and facility access cards of terminated employees are properly disposed of upon collection
- conducting testing to determine whether terminated or transferred employees within our scope retained sensitive access in ATLCloud beyond separation

Generally accepted government auditing 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.