

CHICAGO PARK DISTRICT
OFFICE OF INSPECTOR GENERAL

Revoking Separated
Personnel's Access
to the Chicago Park
District's IT Systems

September 30, 2025



PETER NEUMER | INSPECTOR GENERAL
DANIEL N. LOPEZ | DIRECTOR OF AUDIT

Table of Contents

I. Executive Summary	2
II. Background	4
A. The Identity and Access Management Framework.....	4
B. An Overview of the Chicago Park District’s Personnel	5
C. The Chicago Park District’s Onboarding Process for Granting Access to IT Applications.....	6
III. Objectives, Scope, and Methodology	7
IV. Findings and Recommendations	9
Finding: Structural deficiencies in the Chicago Park District’s offboarding process risks unauthorized access to sensitive information by separated personnel	9
A. The Chicago Park District has insufficient policies and procedures governing access revocation to IT applications for separated personnel.....	10
B. The Chicago Park District cannot establish which personnel has access to which IT applications	12
C. From January 2023 to December 2024, the Chicago Park District notified key departments days to years after personnel separated.....	14
D. The Chicago Park District cannot fully confirm nor otherwise document access revocation for separated personnel.....	19
Finding 1 Recommendations	19
Appendix A: The Joint Department of Human Resources and Department of Information Technology’s Management Response	22
Appendix B: Memo from the Department of Human Resources and Department of Information Technology	29

Acronyms

CISA	Cybersecurity Infrastructure Security Agency
HR	Human Resources
IAM	Identity and Access Management
IT	Information Technology
JML	“Join, Move, Leave” Events of the Workforce
NSA	National Security Agency
OIG	Office of Inspector General

I. Executive Summary

The Office of Inspector General (OIG) conducted an audit of the Chicago Park District's (District) offboarding process to determine if the District timely and appropriately revokes access to the District's IT applications when personnel separate, i.e., end employment.

The OIG found that structural deficiencies in the District's offboarding process risk unauthorized access to sensitive or confidential information by separated personnel. Specifically:

- The District has insufficient policies and procedures governing access revocation to IT applications for separated personnel during the offboarding process;
- The District cannot fully identify all of its personnel, specifically contractors, even though contractors can have access to IT applications;
- The District cannot fully identify all of its IT applications due, in part, to departments being able to independently procure their own applications;
- The District cannot establish which of its personnel has access to which IT applications;
- District IT applications may utilize different credentials; thus, the deactivation of one set of credentials does not revoke access to applications with other credentials;
- The District lacks a standard method for communicating personnel separations;
- Notification to two key departments charged with revoking access for separating personnel may occur anywhere from days to years after the separation, including those who are terminated or designated as ineligible for rehire;
- The District does not inform all relevant departments of personnel separating, specifically those who manage and grant access to certain IT applications;
- The District lacks procedures for identifying when contractors separate, i.e., when a contract expires, and subsequently revoking their access to IT applications;
- The District cannot fully confirm access revocation to IT applications occurs.

These structural deficiencies risk unauthorized access to sensitive or confidential information by separated personnel, including those who have been terminated or are designated as ineligible for rehire.

To address these issues, the OIG recommends the following:

1. The Department of Human Resources and the Department of Information Technology should develop written policies and procedures governing the offboarding process for separated personnel, including those who separate as a result of resignation, retirement, termination, reduction in the workforce, or expiration of a contract. These policies should have specific guidance for coordinating access revocation to the Chicago Park District's IT applications. The Departments should consult with additional departments, as necessary, when creating these policies.

2. The Chicago Park District should consider creating an inventory of all personnel, including contractors and all IT applications, and establish which personnel have access to which applications. If created, this inventory should be reviewed and updated appropriately to ensure timely and valid data.
3. The Chicago Park District should develop policies and implement procedures to ensure all Departments coordinate with the Department of Information Technology when procuring new IT applications.
4. The Chicago Park District should consider working with vendors to establish a single set of credentials across its IT applications, when feasible.
5. The Chicago Park District should implement a standard method for notifying the departments which manage and grant access to IT applications of when personnel, including contractors, separate. The District should further ensure that this method allows for immediate notification of a separation.
6. The Chicago Park District, including the Department of Information Technology, should develop policies and implement procedures to ensure timely and appropriate access revocation to IT applications as well as for documenting and confirming this access revocation.

The Department of Human Resources and Department of Information Technology agreed or agreed in part with each of the OIG's recommendations. The Departments also provided a supplemental memo that sought to provide additional context and detailed its concerns about the OIG's risk assessments, including:

- The term "IT applications" is used in an "overly broad way that implies all systems pose equal risk;"
- The IT application ActiveNet is the only known example identified by the Departments as an application with elevated risks and the Departments have taken steps to mitigate these risks;
- Large employee groups such as lifeguards and attendants only have access to email counts and represent low-risk or informational access;
- All enterprise systems linked to the District's Active Directory are automatically cut off when an account is deactivated; which is centrally managed and tracked in the Department of Information Technology's ticketing system; the higher-risk are department procured systems, "where consistency is hard to enforce;"
- Once a District e-mail account is deactivated, access to shared mailboxes tied to that account is automatically revoked;
- The report does not distinguish between IT contractors and those "engaged by departments under separate agreements;"
- The report's "emphasis on termination dates may give an inflated sense of risk."

For the Department of Human Resources and the Department of Information Technology's full response, *see infra* Appendix A and Appendix B.

II. Background

Chicago Park District personnel, i.e., employees and contractors, are often granted access to the organization's systems, files, and data. These systems, files, and data can contain sensitive or confidential information which, according to best practices, should only be accessible by individuals with appropriate credentials. The following presents an overview, including a framework, for granting and revoking access to systems, including those with sensitive or confidential information.

A. The Identity and Access Management Framework

The National Security Agency (NSA) and the Cybersecurity Infrastructure Security Agency (CISA) state, “[i]dentity and access management (IAM) is a framework of business processes, policies, and technologies that facilitate the management of digital identities to ensure that users only gain access to data when they have the appropriate credentials.”¹ The IAM framework includes several processes to ensure personnel have proper permissions to systems, including:

- Maintaining an inventory of active accounts and privileges;
- Creating policies and rules for segregation of duties requirements;
- Auditing and tracking personnel's permissions and access.²

These processes are part of the IAM framework known as identity governance. Identity governance is:

the process by which an organization centralizes orchestration of its user and service accounts management in accordance with their policies. Identity governance provides organizations with better visibility to identities and access privileges, along with better controls to detect and prevent inappropriate access. It is comprised of a set of processes and policies that cover the segregation of duties, role management, logging, access review, analytics, and reporting.³

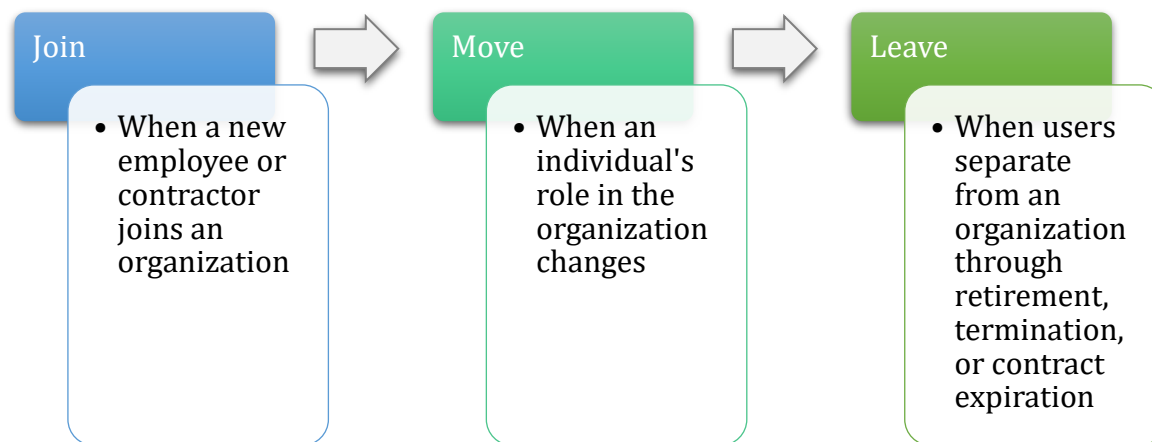
¹ National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

² National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

³ National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

Specifically, identity governance involves the lifecycle of the workforce known as “Join, Move, and Leave” (JML) events (see Figure 1):⁴

FIGURE 1: “JOIN, MOVE, AND LEAVE” (JML) EVENTS OF THE WORKFORCE



Source: OIG analysis of the NSA and CISA's “Recommended Best Practices For Administrators Identity and Access Management.”⁵

Regarding the last major event of the JML lifecycle, “Leave,” the NSA and CISA state, “when users separate from an organization through retirement, termination, or contract expiration, *their accounts and privileges must be promptly terminated* (emphasis added).”⁶

B. An Overview of the Chicago Park District's Personnel

The District employs four types of individuals: full-time employees, part-time employees, seasonal employees, and contractors:

- *Full-Time Employees*
Examples of full-time employees include, but are not limited to, park supervisors, analysts, and legal staff;

[1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF](https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF).

⁴ National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025,

https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

⁵ National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025,

https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

⁶ National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025,

https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

- *Part-Time Employees*
Examples of part-time employees include, but are not limited to, instructors, facilitators, and lifeguards;
- *Seasonal Employees*
Examples of seasonal employees include, but are not limited to, camp counselors and recreation leaders for day camps;
- *Contractors*
Contractors may perform a variety of duties, dependent on the need of the hiring department, such as aiding in management of the District's information technology.

As of December 2024, the District employed approximately 3,000 full-time and part-time employees and, annually, the District employs another approximately 3,000 seasonal employees.

C. The Chicago Park District's Onboarding Process for Granting Access to IT Applications

The District utilizes different information technology applications (IT applications or applications), such as applications available via Microsoft, Oracle, and SharePoint, to help manage the District's operations. According to the Department of Information Technology (IT Department), the onboarding process (the "Join" in the JML events) is generally the same for full-time employees, part-time employees, seasonal employees, and contractors as it pertains to granting access to IT applications. When new personnel are onboarded, the Department of Human Resources (HR Department) and the hiring department provide the IT Department with the new personnel's name, employee number, and title. The hiring department also requests hardware for the new personnel, e.g., desktop, laptop, etc., and certain IT applications including Oracle and Microsoft Office applications. All personnel, including seasonal employees, receive Active Directory credentials which can be used for computer log-ins and e-mail access; however, even though seasonal employees receive these credentials, they may not gain access to applications, e.g., e-mail, because they do not utilize these applications in their roles (*see infra* Finding Section B.2. for more information about Active Directory credentials). Departments can also request that their personnel receive access to additional, specific applications. Upon receiving the request, an IT technician creates a user account utilizing the appropriate license (*see infra* Finding Section B.2 for more information).

III. Objectives, Scope, and Methodology

A. Objective

The objective of this audit was to determine if the Chicago Park District timely and appropriately revokes access to the District's IT applications when personnel separate from the District.

B. Scope

The scope of this audit included the policies and procedures of the Department of Information Technology, the Department of Human Resources, and the Department of Shared Financial Services specifically regarding revoking access to IT applications for separated full-time employees, part-time employees, and contractors. The scope considered policies, procedures, and relevant activities from January 2023 to December 2024. This audit did not evaluate or otherwise review any potential access revocation for seasonal employees as they typically do not receive access to IT applications. This audit further did not evaluate or otherwise review any other offboarding steps for any District employee or contractor, e.g., exit interviews, returning of District property, etc. Finally, this audit did not evaluate or otherwise review unauthorized access to the District's IT applications by third parties.

C. Methodology

The OIG utilized the following methodology to conduct this audit:

- Interviewed personnel from the Department of Information Technology, the Department of Human Resources, and the Department of Shared Financial Services;
- Reviewed policies and procedures from the Department of Information Technology, the Department of Human Resources, and the Department of Shared Financial Services;
- Analyzed 101 termination reports from January 2023 to December 2024, including calculating the length of time of the record termination, i.e., separation, date and the corresponding notification date to the Department of Information Technology, the Department of Human Resources, and the Department of Shared Financial Services.

D. Standards

The OIG conducts performance audits with guidance from the United States Government Accountability Office's Generally Accepted Government Auditing Standards (GAGAS or "Yellow Book," 2024 revision). Pursuant to the Yellow Book:

Performance audits provide objective analysis, findings, and conclusions to assist management and those charged with governance and oversight with, among other things, improving program performance and operations, reducing costs, facilitating decision making by parties

responsible for overseeing or initiating corrective action, and contributing to public accountability.⁷

For other categories of work-product, such as advisories, explainers, notifications, and program descriptions, the Department follows the guidance set forth by the Association of Inspectors General in *Principles and Standards for Offices of Inspector General* ("Green Book," 2024 revision).⁸

E. Authority

The authority to perform this audit is established in Chapter II(D)(4) of the Chicago Park District Code, which states that the OIG has the power and duty to "promote economy, efficiency, effectiveness and integrity in the administrations of programs and operations of the District by reviewing programs, identifying any inefficiencies, waste and potential for misconduct therein, and recommending policies and methods for the elimination of inefficiencies and waste, and for the prevention of misconduct" and "audit and review the District's policies, procedures, functions, and programs."

⁷ United States Government Accountability Office, "Government Auditing Standards 2024 Revisions," February 2024, accessed August 25, 2025, <https://www.gao.gov/assets/d24106786.pdf>.

⁸ Association of Inspectors General, "Principles and Standards for Offices of Inspector General," July 1, 2024, accessed August 25, 2025, <https://inspectorsgeneral.org/blog/newly-revised-aig-green-book-principles-and-standards-for-offices-of-inspector-general-is-now-available-for-download/>.

IV. Finding and Recommendations

Structural deficiencies in the Chicago Park District's offboarding process risks unauthorized access to sensitive information by separated personnel

The Chicago Park District cannot ensure personnel have their access revoked to the District's IT applications, including those with sensitive or confidential information such as customer data, when separating from the District. This is the result of structural deficiencies in the District's offboarding process where decentralization and a lack of coordination is exacerbated by insufficient policies and procedures, ineffective processes, and the absence of a complete understanding of all application users and existing IT applications. Specifically:

- The District has insufficient policies and procedures governing access revocation to IT applications for separated personnel during the offboarding process;
- The District cannot fully identify all of its personnel, specifically contractors, even though contractors can have access to IT applications;
- The District cannot fully identify all of its IT applications due, in part, to departments being able to independently procure their own applications;
- The District cannot establish which of its personnel has access to which IT applications;
- District IT applications may utilize different credentials; thus, the deactivation of one set of credentials does not revoke access to applications with other credentials;
- The District lacks a standard method for communicating personnel separations;
- Notification to two key departments charged with revoking access for separating personnel may occur anywhere from days to years after the separation, including those who are terminated or designated as ineligible for rehire;
- The District does not inform all relevant departments of personnel separating, specifically those who manage and grant access to certain IT applications;
- The District lacks procedures for identifying when contractors separate, i.e., when a contract expires, and subsequently revoking their access to IT applications;
- The District cannot fully confirm access revocation to IT applications occurs.

These structural deficiencies risk unauthorized access to sensitive or confidential information by separated personnel, including those who have been terminated or are designated as ineligible for rehire.

A. The Chicago Park District has insufficient policies and procedures governing access revocation to IT applications for separated personnel

The NSA and CISA IAM framework lists an entity's policies as a factor which helps "ensure that users only gain access to data when they have the appropriate credentials."⁹ These policies can establish processes that are "designed to link people, applications, data, and devices and allow [organizations] to determine who has access to what, what kind of risk that represents, and take action in situations where policy violations are identified."¹⁰ Specifically, the framework instructs organizations to centralize "orchestration of its user and service accounts management in accordance with their policies... that cover the segregation of duties, role management, logging, access review, analytics, and reporting."¹¹

1. The Department of Human Resources' "Policy and Procedure Manual"

The HR Department's "Policy and Procedure Manual" (Manual), last updated February 2019, contains guidance for when personnel separate, specifically in the case of employee resignation and employee termination. For resignations, the Manual states, "[t]he hiring department is responsible for notifying the IT [D]epartment of the employee resignation on the employee[']s last day of work." The HR Department stated it treats retirements like a resignation because in both instances, it is the employee's decision to separate.¹² For terminations, unlike resignations and retirements, the Manual states the HR Department will notify the IT Department "prior to the employee being notified of termination" and that the IT Department "will be responsible for denying the employee access to log in the computer and access to voice mail."

Although the Manual states, "[i]t is the policy of the [District] to separate employment because of an employee's resignation, termination and retirement, the expiration of an employment contract or a reduction in the work force," the Manual does not provide

⁹ National Security Agency and the Cybersecurity Infrastructure Security Agency, "Recommended Best Practices For Administrators Identity and Access Management," March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

¹⁰ National Security Agency and the Cybersecurity Infrastructure Security Agency, "Recommended Best Practices For Administrators Identity and Access Management," March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

¹¹ National Security Agency and the Cybersecurity Infrastructure Security Agency, "Recommended Best Practices For Administrators Identity and Access Management," March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

¹² The HR Department noted, from the Department's perspective, the only factor that differentiates a resignation from a retirement is that the latter requires the Department to inform the retiring employee of additional information, such as Medicare.

guidance for offboarding personnel due to a contract expiration or work force reduction. In the case of resignations (and retirements), the Manual contradicts the actual process where the HR Department, rather than the hiring department, generally notifies the IT Department (*see infra* Section C, below, for more information). However, the Manual does not establish a specific process for the HR Department or a hiring department to notify the IT Department about a resignation (or retirement) or reference revoking access to IT applications for any separation, e.g., resignation, termination, etc.¹³

2. The Department of Information Technology's Policies

The IT Department has two policies, created over a decade ago, related to the IAM framework: Policy Number 1200.28 "Chicago Park District IT Security" from December 2007 and the "IT Security Policy," marked as draft, from October 2012. Both of these policies include the same language regarding "unauthorized access, accidental or deliberate, to the Park District's sensitive and confidential information," specifically:

Security standards are necessary for the protection of Chicago Park District information. The goals of the security program are to provide for the following:

(1) Active prevention of the unauthorized access, accidental or deliberate, to the Park District's sensitive and confidential information.

(2) Adequate protection of Park District sensitive and confidential information against accidental or deliberate modification or destruction to include a combination of direct protection of the information and its storage media, enforcement of associated discretionary need-to-know practices and redundancy through backup information collected.

(3) Timely detection of the unauthorized access attempts of the Park District's sensitive and confidential information.

(4) Timely and accurate damage assessment following either the detection of the physical entrance to an information processing facility or the unauthorized access to the Park District's sensitive and confidential information.

(5) Orderly recovery of information systems processing capabilities as a result of either an unauthorized access or physical damage.

Likewise, both policies state:

¹³ As noted above, the Manual does state, "[the] IT [Department] will be responsible for denying the employee access to log in on the computer and access to voice mail."

When an employee is transferred or terminated, the employee's department head or designee must immediately notify the appropriate system administrator to ensure removal of computer user identification codes. The department head or designee must also arrange for the orderly retention or destruction of information files.

Although both of these policies require immediate notification when an employee is transferred or terminated, i.e., separated, neither policy provides specific guidance for the notification process nor any guidance for the "appropriate system administrator" when removing "computer user identification codes."¹⁴

B. The Chicago Park District cannot establish which personnel has access to which IT applications

The District does not know which personnel has access to which IT applications, thus, undermining the District's ability to successfully revoke access for separated personnel to its applications, including those with sensitive or confidential information. As noted in the background section, the IAM framework provides guidance for organizations to ensure personnel have proper permissions when accessing IT applications, including, "maintain[ing] an inventory of active accounts and privileges that currently exist in systems and applications."¹⁵ According to the NSA and CISA, this guidance for "centralized control and visibility helps to mitigate the risk that identities and privileges will be mismanaged [and] enable[e] administrators to identify and remove non-compliant combinations of privileges assigned to individuals."¹⁶ However, according to the IT Department, the District does not maintain such an inventory of which employees and contractors have access to which IT applications, nor does the District have a complete list of all application users or even a complete list of all District IT applications, as discussed below.

¹⁴ The IT Department did not recognize the 2012 policy, marked as draft, nor does the IT Department have other policies in effect governing the offboarding process, specifically for access revocation for separated personnel. The OIG presented the 2012 policy to the IT Department in order to confirm its status, i.e., if the policy was still a draft.

¹⁵ National Security Agency and the Cybersecurity Infrastructure Security Agency, "Recommended Best Practices For Administrators Identity and Access Management," March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

¹⁶ National Security Agency and the Cybersecurity Infrastructure Security Agency, "Recommended Best Practices For Administrators Identity and Access Management," March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

1. The Chicago Park District Personnel

As discussed in the Background Section, the District employs four types of individuals: full-time employees, part-time employees, seasonal employees, and contractors. As of December 2024, the District employed approximately 3,000 full-time and part-time employees and, annually, the District employs another approximately 3,000 seasonal employees. Each of these employees may be granted access to a specific set of IT applications, depending on their role and responsibilities. However, the District does not know how many contractors it has at any given point-in-time nor how many of these contractors have access to the District's IT applications, even though some contractors do have such access. This is due to lack of a central entity managing the District's contractors and contractor information, including start and end dates. This information is instead siloed into many departments. The HR Department stated the Department does not "handle" the District's contractors and, instead, it is the responsibility of individual departments who work with contractors. As of December 2024, the IT Department identified over 3,000 District accounts, including both employees and shared mailboxes, e.g., a single human resources e-mail account that automatically sends an e-mail to multiple HR Department employees, as well as an additional 138 contractors.¹⁷

2. The Chicago Park District IT Applications

As is the case with contractors, the District does not know the complete list of IT applications utilized by District personnel due to similar decentralization. The IT Department stated it has "no visibility" into which applications are purchased independently by another department. Further complicating matters, not all IT applications require the same District employee credentials to log in and access the information stored in the application. For example, the District utilizes an application called ActiveNet used by employees and contractors for financial transactions with District customers, i.e., members of the public. Completely independent from ActiveNet, the District also utilizes a system called Active Directory which creates credentials for District employees. The IT Department manages the Active Directory and the Department of Shared Financial Services (Shared Financial Services) manages ActiveNet. However, ActiveNet does not utilize the credentials created in the Active Directory and instead has its own separate log-in credentials. This means when the IT Department disables the credentials for separated personnel in the Active Directory, it does not automatically disable the separated personnel's account in ActiveNet. Instead, Shared Financial Services must be additionally notified of personnel separating and is subsequently responsible for deactivating these accounts (*see infra* Section C.1 for more

¹⁷ The IT Department noted that once a District e-mail account is deactivated, access to shared mailboxes tied to that account is automatically revoked. However, as is the case with contractors and applications, the District does not have a centralized entity responsible for shared mailboxes. Instead, shared mailboxes are managed by a single individual who may be in a department other than the IT Department and, according to the IT Department, may not even know they are responsible for the shared mailbox. The IT Department stated these individuals have "autonomous power" over the shared mailbox, and can feasibly add a private, i.e., personal, e-mail account to a shared mailbox, and that it is ultimately the individual's responsibility to remove these personal accounts.

information). This situation is not limited to just ActiveNet as the IT Department stated an application not requiring Active Directory credentials “happens often,” which presents a security issue as “anyone can log in” to these IT applications.

Because the District does not know the full universe of IT applications used by personnel, the District cannot fully determine which applications contain sensitive or confidential information. Using ActiveNet as an example of a known application, the application contains information which includes, but is not limited to:

- Customer's name;
- Customer's age and date of birth;
- Customer's gender;
- Customer's personal phone number;
- Customer's work phone number;
- Customer's home address;
- Customer's personal e-mail address;
- Customer's primary contact name;
- The primary contact's phone number;
- The last four digits of the customer's credit or debit card;
- The expiration date of the credit or debit card.

C. From January 2023 to December 2024, the Chicago Park District notified key departments days to years after personnel separated

In addition to not having sufficient policies and procedures governing the offboarding process and lacking an inventory of users and their respective access to IT applications, the District does not notify key departments of separations, and thus does not ultimately revoke access, in a timely manner. As noted in the Background section, the NSA and CISA state, “when users separate from an organization through retirement, termination, or contract expiration, their accounts and privileges must be *promptly* terminated” (emphasis added).¹⁸ From January 2023 to December 2024, the average length of time between when an individual was separated to when the IT Department was informed of their separation ranged between 1.2 and 2.1 months with a maximum length of 3.1 years (the average range corresponds to two subsets of employees, as discussed below; *see infra* Section C.2).

1. Weekly Termination Reports

The District's primary method for communicating the separation of personnel for the purposes of revoking IT application access is the weekly termination report. The process for

¹⁸ National Security Agency and the Cybersecurity Infrastructure Security Agency, “Recommended Best Practices For Administrators Identity and Access Management,” March 21, 2023, accessed August 25, 2025, https://media.defense.gov/2023/Mar/21/2003183448/-1/-1/0/ESF%20IDENTITY%20AND%20ACCESS%20MANAGEMENT%20RECOMMENDED%20BEST%20PRACTICES%20FOR%20ADMINISTRATORS%20PP-23-0248_508C.PDF.

separating employees, as it relates to access revocation, begins when the HR Department’s Employment Services Manager receives an Employee Action Form (Form 166), a generic form used to document any change in employment, including separation. Although the form is to be submitted when personnel separate, the HR Department stated they do not always receive a notification of separation. For example, the Employment Services Manager stated they are sometimes made aware of a separation because a manager will inquire why a separated employee is still included in payroll for the manager’s approval; the Employee Services Manager stated this is because the HR Department was never made aware of the employee’s separation. According to the Manager, this delay in notification can be weeks or months after the separation. Further, the Form 166 is not always completed upon submission, sometimes resulting in the omission of information including the “termination action,” e.g., resignation, fired, etc., and whether the separated personnel are recommended for rehire. When the HR Department does receive notice of separation, either via the Form 166 or another method, the Employment Services Manager enters this information into an Oracle system, which officially terminates employment with the District.

Once an employee has been separated, they are included in a weekly termination report, a Microsoft Excel file that is generated and automatically disseminated at 10 AM every Monday. Report recipients include personnel in the HR Department, the IT Department, and Shared Financial Services (The District includes Shared Financial Services as a recipient of these reports to revoke access to ActiveNet in order to mitigate access risks, given ActiveNet’s separate credentials).¹⁹ Among other data points, the weekly termination reports include the separated employee’s name, employee number, and termination, i.e., separation, date (see Figure 2, below, for an example of these reports):

FIGURE 2: SELECT DATA FROM THE DECEMBER 09, 2024 TERMINATION REPORT

Employee Number	Full Name	Start Date	Termination Date	Termination Action	Termination Action Reason	Recommended for Rehire	Person Type	Employee Category
			04-Dec-2024	Resignation	Resign Do Not Rehire Tem	Not Specified	EMP	Fulltime Nonexempt
			08-Jul-2024	Termination	Terminated Do Not Rehire	Not Specified	EMP	Hourly Nonexempt
			23-Nov-2024	Resignation	Resignation	Not Specified	EMP	Hourly Nonexempt
			29-Aug-2024	Resignation	Resignation	Not Specified	EMP	Hourly Nonexempt
			06-Nov-2024	Seasonal Terminat	Seasonal - Termination	Not Specified	EMP	Seasonal
			06-Nov-2024	Seasonal Terminat	Seasonal - Termination	Not Specified	EMP	Seasonal
			06-Nov-2024	Seasonal Terminat	Seasonal - Termination	Not Specified	EMP	Seasonal
			06-Nov-2024	Seasonal Terminat	Seasonal - Termination	Not Specified	EMP	Seasonal
			06-Nov-2024	Resignation	Resignation	Not Specified	EMP	Hourly Nonexempt

Source: The Chicago Park District.

As these reports are only generated and disseminated on a weekly basis, i.e., 10 AM every Monday, if an employee was separated on a Tuesday, the soonest the employee could be included in a report would be the following Monday. Upon receipt of the termination reports, the IT Department is to revoke access to the IT applications within the Department’s purview, including deactivating the separated employees’ Active Directory account which,

¹⁹ The District’s Communication Specialist in the Marketing Department is also a recipient; the HR Department was unable to identify why the Specialist receives these reports.

once deactivated, immediately revokes access to certain IT applications, such as Oracle and Microsoft 365, that use Active Directory credentials. This process is centrally managed and tracked via the IT Department's ticketing system. Shared Financial Services is to perform parallel actions for the applications ActiveNet and ActiveWorks, although this Department stated that notifications of separations are not limited to the weekly termination reports and can "come in a lot of different ways" such as e-mails and phone calls.

Further, as discussed above, even though many District departments procure and utilize unique IT applications, some of which are not tied to the Active Directory and also may not be known to the IT Department, the weekly termination reports are only sent to the HR Department, the IT Department, and Shared Financial Services. Therefore, other Departments may not learn of an employee's separation resulting in the separated employee's active access to the application and subsequent data. For example, the Department of Purchasing (Purchasing Department) utilizes an IT application called Bonfire which houses information regarding the District's contracts and has credentials independent of the Active Directory. An OIG employee with access to Bonfire resigned in early January 2025; however, the Purchasing Department inquired about the separation on April 28, 2025, noting they would "like to [d]isable [their] account."

2. Weekly Termination Reports from January 2023 through December 2024

Although the weekly termination reports are sent every Monday, separated employees may be included in a report generated and disseminated anywhere from days to years after their separation date. For example, as previously shown in Figure 2 of the December 9, 2024 termination report, the termination dates range from July 8, 2024 to December 4, 2024. In 101 weekly termination reports from January 2023 through December 2024, over 7,400 individuals were included with the earliest termination date of December 31, 2019. However, these reports include both seasonal employees who, generally, do not receive access to IT applications, including e-mail accounts, as well as duplicate inclusions, i.e., individuals who are included multiple times across different reports.

When excluding seasonal employees and employees with duplicative inclusions, the number of separated employees decreases to 674, a number, when evenly distributed across both years in consideration, represents approximately 11% of the District's annual non-seasonal workforce. Regarding this subset, the average length of time from when the employee was separated to when they were included in a weekly termination report was 2.1 months (see Table 1 and 2 for more information; note: months assume a 30-day period). It is important to note, as notifications of separations are not exclusively communicated via these reports, as discussed above, it is possible the IT Department and other departments may have been notified sooner in some cases, via an alternative form of communication such as a phone call or e-mail. The information presented below reviews the District's primary form of communication, i.e., the weekly termination report, when notifying about separations.

TABLE 1: DESCRIPTIVE STATISTICS REGARDING THE LENGTH OF TIME BETWEEN TERMINATION DATES AND INCLUSION IN A WEEKLY TERMINATION REPORT, JANUARY 2023 TO DECEMBER 2024

	Days	Weeks	Months	Years
Mean	62.7	9.0	2.1	0.2
Median	19.0	2.7	0.6	0.1
Max	1,125.0	160.7	37.5	3.1
Min	1.0	0.1	0	0

Source: OIG analysis of the Chicago Park District’s weekly termination reports, January 2023 to December 2024.

TABLE 2: COUNT OF SEPARATED EMPLOYEES BY LENGTH OF TIME BETWEEN TERMINATION DATE AND INCLUSION IN A WEEKLY TERMINATION REPORT, JANUARY 2023 TO DECEMBER 2024

	Count	Percent
Greater than 1 Day	673	99.9%
Greater than 1 Week	581	86.2%
Greater than 1 Month	196	29.1%
Greater than 1 Year	33	4.9%
Greater than 2 Years	2	0.3%
Greater than 3 Years	1	0.1%

Source: OIG analysis of the Chicago Park District’s weekly termination reports, January 2023 to December 2024.

Additionally, of these 674 employees, 101 (15.0%) were designated as ineligible for rehire, with 88 employees taking longer than one week to appear on a weekly termination report, 41 longer than a month, and 10 longer than a year.

Regarding duplicate inclusions, i.e., separated employees who appear in multiple weekly termination reports, neither the HR Department nor the IT Department could confirm why this occurs.²⁰ Therefore, the OIG is considering these employees a separate subset from the employees discussed above. When excluding seasonal employees, an additional 132 employees appear in the reports disseminated between January 2023 and December 2024, which when combined with the previous set of 674 employees, represents approximately 13% of the annual non-seasonal workforce. The average length of time in this second subset from when an employee was separated to when they were first included in a weekly termination report was 1.2 months (see Table 3 and 4 for more information; note: months assume a 30-day period).²¹

²⁰ During fieldwork, the HR Department hypothesized that duplicate inclusions could be the result of changes in the Oracle system where anytime a data field pertaining to a separated employee is edited, this action automatically results in Oracle including the separated employee as a new entry in a new weekly termination report. After fieldwork, the HR Department confirmed, in consultation with the IT Department, this was the case.

²¹ The OIG analyzed the weekly termination data for duplicate inclusions by only considering when a separated employee first appeared in a weekly termination report. This decision was informed by the HR Department’s

TABLE 3: DESCRIPTIVE STATISTICS FOR DUPLICATIVE INCLUSIONS REGARDING THE LENGTH OF TIME BETWEEN TERMINATION DATES AND INCLUSION IN A WEEKLY TERMINATION REPORT, JANUARY 2023 TO DECEMBER 2024

	Days	Weeks	Months	Years
Mean	37.4	5.3	1.2	0.1
Median	17.0	2.4	0.6	0.0
Max	1,119.0	159.9	37.3	3.1
Min	0.0	0.0	0	0

Source: OIG analysis of the Chicago Park District’s weekly termination reports, January 2023 to December 2024.

TABLE 4: COUNT OF SEPARATED EMPLOYEES WITH DUPLICATIVE INCLUSIONS BY LENGTH OF TIME BETWEEN TERMINATION DATE AND INCLUSION IN A WEEKLY TERMINATION REPORT, JANUARY 2023 TO DECEMBER 2024

	Count	Percentage
Greater than 1 Day	129	97.7%
Greater than 1 Week	98	74.2%
Greater than 1 Month	28	21.2%
Greater than 1 Year	2	1.5%
Greater than 2 Years	1	0.8%
Greater than 3 Years	1	0.8%

Source: OIG analysis of the Chicago Park District’s weekly termination reports, January 2023 to December 2024.

Additionally, of these 132 other employees, 37 (28.0%) were designated as ineligible for rehire, with 29 employees taking longer than one week to appear on a weekly termination report, 9 longer than a month, and no employees for longer than a year.

The HR Department, recognizing the long lead times between termination dates and the IT Department being notified, introduced a Microsoft Form entitled “Exit Notification (Advance Notice for IT)” in January 2025. Upon learning of a pending separation, the HR Department is supposed to complete the form which, in turn, automatically updates a list of separated employees which can be generated in a Microsoft Excel file. This form is intended to be a temporary solution until the District updates an Oracle system to include a field for a pending termination; the HR Department stated that this Oracle update would “complement” the weekly termination reports.

3. Contractor Separation

Contractors are not included in weekly termination reports, even though contractors can have access to the District’s IT applications. The HR Department stated contractors are not included because they are not officially District employees. The IT Department stated it would need to be informed directly by a user department when a contractor separates, i.e.,

then-hypothesis described in the previous footnote; however, it is possible other valid explanations could exist for the duplicative entries, such as an employee separating, returning to employment, and then separating a second time.

when a contract expires, otherwise, the IT Department “would not know.” Due to this lack of coordination and communication, the OIG cannot review if or when the District is made aware of contractors separating or when the IT Department or other relevant departments, e.g., Shared Financial Services, are notified.

D. The Chicago Park District cannot fully confirm nor otherwise document access revocation for separated personnel

Weekly termination reports only serve as a mechanism to inform select District departments of separations; they do not confirm access revocation to IT applications. The IT Department stated they do not document access revocation once the Department receives the weekly reports. Further, the IT Department does not confirm with the HR Department or with a separated employee's department that the employee's access to certain IT applications have been revoked. Shared Financial Services does maintain a Microsoft Excel spreadsheet which lists the dates the Department revoked access to ActiveNet, but they do not confirm this revocation with the HR Department or with the separated employee's department. Further, it is unclear how or if other departments document or confirm access revocation of applications which they manage, e.g., the Purchasing Department and their Bonfire application. Due to these factors, the OIG cannot fully confirm if access revocation has occurred for any separated personnel, but, critically, neither can the District.

Recommendations

1. The Department of Human Resources and the Department of Information Technology should develop written policies and procedures governing the offboarding process for separated personnel, including those who separate as a result of resignation, retirement, termination, reduction in the workforce, or expiration of a contract. These policies should have specific guidance for coordinating access revocation to the Chicago Park District's IT applications. The Departments should consult with additional departments, as necessary, when creating these policies.
2. The Chicago Park District should consider creating an inventory of all personnel, including contractors and all IT applications, and establish which personnel have access to which applications. If created, this inventory should be reviewed and updated appropriately to ensure timely and valid data.
3. The Chicago Park District should develop policies and implement procedures to ensure all Departments coordinate with the Department of Information Technology when procuring new IT applications.
4. The Chicago Park District should consider working with vendors to establish a single set of credentials across its IT applications, when feasible.
5. The Chicago Park District should implement a standard method for notifying the departments which manage and grant access to IT applications of when personnel, including contractors, separate. The District should further ensure that this method allows for immediate notification of a separation.

6. The Chicago Park District, including the Department of Information Technology, should development policies and implement procedures to ensure timely and appropriate access revocation to IT applications as well as for documenting and confirming this access revocation.

Management Response

The Department of Human Resources and Department of Information Technology agreed or agreed in part with each of the OIG's recommendations. The Departments also provided a supplemental memo in response to the OIG's draft report containing the following:

"As noted in our formal Management Response Form, HR and IT agree with the recommendations to strengthen offboarding. We also want to provide context that clarifies where risk is most concentrated and where the draft report may have overstated exposure.

1. Definition of 'IT applications'

The draft uses the term "IT applications" in an overly broad way that implies all systems pose equal risk. In practice, the District's large-scale Enterprise Applications (HCM, ERP, EAM, BI, email, file storage, conferencing, etc.) are centrally managed by IT, with access revocations routed through the ticketing system and tracked. By contrast, department-procured or non-SSO applications are not always within IT's direct management, and controls can vary.

2. ActiveNet as an Outlier

The draft highlights ActiveNet as a risk example and frames it as though the gap was unaddressed or indicative of a broader pattern. In reality, Finance and IT were already aware of ActiveNet's separate credentials and took steps to mitigate the risk by including Finance in the termination reporting process. Finance and IT had also been exploring options for SSO integration prior to the audit and are moving toward implementation. While the draft cites an IT comment that non-SSO exposure 'happens often,' this should not be read as evidence of other ActiveNet-like systems. In practice, most non-SSO systems are low-risk tools for internal tracking, scheduling, or work orders that do not store sensitive information. ActiveNet remains the only known example with elevated risk, and Finance supplements controls with annual account audits.

3. Low-Risk Email Accounts

Large employee groups such as Lifeguards, Security Guards, Trades staff, and most Recreation Leaders and Attendants had only District email accounts, used primarily for communication and scheduling. These accounts represent low-risk or informational access and were not used to transmit or handle sensitive or confidential information.

4. Current Risk and Revocation Controls

For enterprise applications, access revocation is routed through IT's ticketing system and subject to established controls. All enterprise systems linked to Active Directory are automatically cut off when an account is deactivated, which is centrally managed and tracked in IT's ticketing system. Delays in how separations were communicated to IT did create gaps in timeliness, but these primarily affected staff with only email or other low-risk access. Once IT is notified, revocation is executed promptly and documented. The higher-risk exposure is with department-procured systems, where consistency is harder to enforce. Without drawing this distinction, the draft overstates the exposure of the District's most sensitive systems.

5. Shared mailboxes

The draft misinterprets how shared mailbox access functions. Once a District email account is deactivated, access to shared mailboxes tied to that account is automatically revoked. While some departments manage mailbox permissions, these permissions cannot persist once the underlying District account is disabled.

6. Contractors

The draft does not distinguish between IT contractors, who are centrally managed with established controls, and contractors engaged by departments under separate agreements. IT tracks, monitors, and offboards its own contracted employees. By contrast, most other contractors are independent and perform their services without requiring access to District systems. Where contractors did have access, such as ActiveNet, permissions were limited to specific functions, and Finance supplements this with annual audits to confirm inactive accounts are removed.

7. Termination Dates in Section IV(C)

The report's emphasis on termination dates may give an inflated sense of risk. Even after excluding seasonal employees and duplicates, the focus on the 674 remaining employees conflates reporting lag with actual access risk. Most had only low-risk, informational email accounts, and the majority did not have ActiveNet accounts. Of the few who did, Finance was already engaged in monitoring access through the termination reporting process.

As previously confirmed with IT Applications, the weekly termination report reflects updates made in Oracle, meaning separated employees can reappear if fields are later corrected (for example, a rehire designation). This reporting mechanic helps explain the apparent over-representation of late-appearing "Do Not Rehire" employees. For employees with access to sensitive enterprise systems, HR coordinated directly with IT to ensure access was cut off promptly. For these reasons, the date of appearance on a termination report is not a reliable indicator of timeliness of access revocation."

For the Department of Human Resources and the Department of Information Technology's full response, *see infra* Appendix A and Appendix B.

Appendix A: The Joint Department of Human Resources and Department of Information Technology's Management Response

Recommendation 1			
<p>The Department of Human Resources and the Department of Information Technology should develop written policies and procedures governing the offboarding process for separated personnel, including those who separate as a result of resignation, retirement, termination, reduction in the workforce, or expiration of a contract.</p> <p>These policies should have specific guidance for coordinating access revocation to the Chicago Park District's IT applications.</p> <p>The Departments should consult with additional departments, as necessary, when creating these policies.</p>			
Department Response	Agree <input checked="" type="checkbox"/>	Agree, in part <input type="checkbox"/>	Disagree <input type="checkbox"/>
Notes on Department Response			
<p>We agree that formal written policies and procedures are needed to ensure consistency and accountability in the offboarding process. While HR and IT already coordinate directly on certain sensitive separations, a documented process will clarify expectations, roles, and timelines across all types of separations.</p>			
Department's Proposed Corrective Action (if in agreement with Recommendation)			
<p>HR and IT will jointly draft offboarding policies and procedures. These will include guidance on notification protocols, documentation requirements, and timelines for revoking system access.</p> <p>Draft Policy Direction The joint policy will set clear expectations for department-procured applications:</p> <ul style="list-style-type: none"> • Any application or portal that (1) contains sensitive or confidential information, (2) provides transactional authority, or (3) grants access across multiple departments must either be integrated with Single Sign-On (SSO) or have a designated system administrator on the Projected Termination Report distribution list. • System administrators receiving notifications will be responsible for revoking access promptly and maintaining a record of deprovision dates. • All other department-controlled applications or portals may remain locally managed, provided department heads maintain current user lists and ensure access is removed when staff separate. 			

Implementation Time Frame	Drafting and initial rollout: by end of Q1 2026. Final approval and integration: by mid-2026.
Responsible Party(ies) for Implementation	IT and HR

Recommendation 2			
<p>The Chicago Park District should consider creating an inventory of all personnel, including contractors and all IT applications, and establish which personnel have access to which applications.</p> <p>If created, this inventory should be reviewed and updated appropriately to ensure timely and valid data.</p>			
Department Response	Agree <input type="checkbox"/>	Agree, in part <input checked="" type="checkbox"/>	Disagree <input type="checkbox"/>
Notes on Department Response			
<p>We agree that a centralized inventory is needed, but it should be scoped and risk-based. A full inventory of all department-procured applications is not practical or necessary, as many applications pose no risk (for example, applications used only for internal tracking or non-sensitive data). The first step will be to scope and prioritize which applications and contractors actually require inclusion, focusing on those with sensitive information, transactional authority, or cross-departmental use.</p> <p>For contractors, the inventory should be limited to those who are known to have system access, rather than all contractors engaged by the District.</p> <p>Implementation will require outreach to department heads to identify which applications are in use. IT will then review these to determine which fall into scope (non-SSO, sensitive/confidential, transactional, or cross-departmental). Vendor discussions will follow to verify capabilities and identify system administrators. This is a multi-step process that will require a longer timeline.</p>			
Department's Proposed Corrective Action (if in agreement with Recommendation)			
<p>IT will first conduct a scoping exercise to identify department-procured applications and contractors known to have system access. As part of this review, we will also identify the designated system administrator for each application. Based on this review, we will develop a centralized inventory for applications that:</p> <ul style="list-style-type: none"> • Are not integrated with SSO, and 			

<ul style="list-style-type: none"> • Contain sensitive or confidential information, or • Grant transactional authority, or • Provide access across multiple departments. <p>For department-controlled applications outside of this scope, departments will continue to manage access locally, but will be expected to maintain user lists, designate a system administrator, and ensure timely removal of access when staff separate.</p>	
Implementation Time Frame	Initial outreach and assessment with department heads: by Q1 2026. Vendor validation and administrator identification: by Q2 2026. Ongoing updates: annually, or as new applications or portals are identified.
Responsible Party(ies) for Implementation	IT

Recommendation 3	
The Chicago Park District should develop policies and implement procedures to ensure all Departments coordinate with the Department of Information Technology when procuring new IT applications.	
Department Response	Agree <input type="checkbox"/> Agree, in part <input checked="" type="checkbox"/> Disagree <input type="checkbox"/>
Notes on Department Response	
We agree that IT should be involved in the procurement process for new applications where risk is significant, such as applications or portals that handle sensitive or confidential information, provide transactional authority, or grant access across multiple departments. However, we do not believe it is necessary or practical for IT to be involved in every departmental procurement of low-risk tools or applications that are used and managed locally without sensitive data.	
Department's Proposed Corrective Action (if in agreement with Recommendation)	
The IT team will create a policy that will require Departments to coordinate with the IT team. The teams can then collectively review any applications that they intend to procure that would host or interact with sensitive or confidential data. Within this policy there will also be requirements as to how user access will be managed and monitored. Every new application that is procured (and hosts or interacts with sensitive data) and has the capability of integrating SSO will coordinate with the IT infrastructure team to ensure compliance. If the application does not have SSO capabilities the team will work with the user department to implement an offboarding process for user access.	

Implementation Time Frame	Draft policy framework: by Q1 2026. Finalize and roll out process: by mid-2026.
Responsible Party(ies) for Implementation	IT

Recommendation 4

The Chicago Park District should consider working with vendors to establish a single set of credentials across its IT applications, when feasible.

Department Response Agree Agree, in part Disagree

Notes on Department Response

We agree with the value of expanding single sign-on (SSO) integration where feasible. Centralized credentials improve security and simplify offboarding by allowing IT to deactivate multiple applications through one control point. However, we recognize that not all vendor applications currently support SSO, and some department-procured applications are low-risk and may not warrant the investment required for integration.

Establishing a single set of credentials across applications depends on vendors' ability to support Single Sign-On (SSO). We will need time to assess each application, determine feasibility, and then work with vendors and IT to configure and implement. This is a multi-step process that will require a longer timeline.

Department's Proposed Corrective Action (if in agreement with Recommendation)

The Information Technology team will meet with departments to identify and review if applications are suitable for SSO, prioritizing those that:

- Contain sensitive or confidential information,
- Provide transactional authority, or
- Are used across multiple departments.

Applications that cannot feasibly be integrated into SSO will remain locally managed, with department system administrators required to ensure timely offboarding.

Implementation Time Frame	Assessment phase with departments: Q1-Q2 2026.
----------------------------------	------------------------------------------------

	Vendor engagement and integration: system-by-system, 6+ months depending on vendor capability.
Responsible Party(ies) for Implementation	IT

Recommendation 5

The Chicago Park District should implement a standard method for notifying the departments which manage and grant access to IT applications of when personnel, including contractors, separate.

The District should further ensure that this method allows for immediate notification of a separation.

Department Response Agree Agree, in part Disagree

Notes on Department Response

We agree that a standardized notification method is needed. At the commencement of the audit, the weekly termination report was the primary method, supplemented by direct HR-IT communication for sensitive separations. Since then, HR has implemented a new projected termination report that provides advance notice of upcoming separations.

Department's Proposed Corrective Action (if in agreement with Recommendation)

Since the audit period, HR has implemented a new Projected Termination Report that provides advance notice of upcoming separations. This report is already distributed to IT and Finance for deprovisioning purposes and allows action to be scheduled for the effective termination date.

Next steps will include:

- Expanding the distribution list to ensure system administrators of non-SSO applications with sensitive information are notified.
- Formalizing protocols for urgent or same-day separations to supplement the weekly report.
- Documenting these steps in the joint HR-IT offboarding policy.

Implementation Time Frame	Projected Termination Report implemented. Refinements (distribution list expansion, urgent separation protocols): by early 2026.
----------------------------------	-------------------------------------------------------------------------------------------------------------------------------------

Responsible Party(ies) for Implementation	HR and IT
--------------------------------------------------	-----------

Recommendation 6

The Chicago Park District, including the Department of Information Technology, should develop policies and implement procedures to ensure timely and appropriate access revocation to IT applications as well as for documenting and confirming this access revocation.

Department Response	Agree <input type="checkbox"/>	Agree, in part <input checked="" type="checkbox"/>	Disagree <input type="checkbox"/>
----------------------------	--------------------------------	----------------------------------------------------	-----------------------------------

Notes on Department Response

All enterprise applications containing sensitive or confidential data already have processes in place to revoke access and IT maintains documentation of these actions. However, revocation was not always timely, particularly when separation was not communicated immediately. To address this, HR has implemented a projected termination report that is distributed weekly to IT and Shared Financial Services, providing advance notice of separations. This step reduces the delay between separation and revocation, but additional work is needed to improve consistency across all applications.

Ensuring timely and documented access revocation requires first identifying all department-procured or non-SSO applications containing sensitive information, then coordinating with application owners to integrate into the projected termination process or establish parallel procedures. This will require department meetings and vendor coordination, which will extend the implementation timeframe.

Department's Proposed Corrective Action (if in agreement with Recommendation)

Determine what other department-procured or non-SSO applications exist that house sensitive information, identify the system administrator for each, and ensure they are added to the projected termination report distribution list so revocations can be executed and confirmed promptly. HR and IT will develop written offboarding policies to reflect notification protocols, documentation requirements, and timelines for revoking access.

Implementation Time Frame	<p>Policy drafting and approval: by Q2 2026 (aligned with Rec 1). Process alignment and distribution list updates: Q2-Q3 2026. Full rollout and training: by end of 2026.</p>
----------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Responsible Party(ies) for Implementation	HR and IT
--------------------------------------------------	-----------

Appendix B: Memo from the Department of Human Resources and Department of Information Technology



Administration Office
4830 S. Western Avenue
Chicago, Illinois 60609
(312) 742-7529
www.chicagoparkdistrict.com

Board of Commissioners

Dr. Marlon Everett
President

Modesto Valle
Vice President

Coya Paz Brownrigg
Sharon Bush
Robert Castaneda
Sean Garrett
Philip Jackson

**General Superintendent
& CEO**
Carlos Ramirez-Rosa

City of Chicago
Brandon Johnson
Mayor

Memo

To: Office of the Inspector General – Audit
From: Department of Human Resources and Department of Information Technology
Date: September 29, 2025
Re: Management Response – Supplemental Narrative

As noted in our formal Management Response Form, HR and IT agree with the recommendations to strengthen offboarding. We also want to provide context that clarifies where risk is most concentrated and where the draft report may have overstated exposure.

1. Definition of "IT applications"

The draft uses the term "IT applications" in an overly broad way that implies all systems pose equal risk. In practice, the District's large-scale Enterprise Applications (HCM, ERP, EAM, BI, email, file storage, conferencing, etc.) are centrally managed by IT, with access revocations routed through the ticketing system and tracked. By contrast, department-procured or non-SSO applications are not always within IT's direct management, and controls can vary.

2. ActiveNet as an Outlier

The draft highlights ActiveNet as a risk example and frames it as though the gap was unaddressed or indicative of a broader pattern. In reality, Finance and IT were already aware of ActiveNet's separate credentials and took steps to mitigate the risk by including Finance in the termination reporting process. Finance and IT had also been exploring options for SSO integration prior to the audit and are moving toward implementation. While the draft cites an IT comment that non-SSO exposure "happens often," this should not be read as evidence of other ActiveNet-like systems. In practice, most non-SSO systems are low-risk tools for internal tracking, scheduling, or work orders that do not store sensitive information. ActiveNet remains the only known example with elevated risk, and Finance supplements controls with annual account audits.

3. Low-Risk Email Accounts

Large employee groups such as Lifeguards, Security Guards, Trades staff, and most Recreation Leaders and Attendants had only District email accounts, used primarily for communication and scheduling. These accounts represent low-risk or informational access and were not used to transmit or handle sensitive or confidential information.

4. Current Risk and Revocation Controls

For enterprise applications, access revocation is routed through IT's ticketing system and subject to established controls. All enterprise systems linked to Active Directory are automatically cut off when an account is deactivated, which is centrally managed and tracked in IT's ticketing system. Delays in how separations were communicated to IT did create gaps in timeliness, but these primarily affected staff with only email or other low-risk access. Once IT is notified, revocation is executed promptly and documented. The higher-risk exposure is with department-procured systems, where consistency is harder to enforce. Without drawing this distinction, the draft overstates the exposure of the District's most sensitive systems.

6. Shared mailboxes

The draft misinterprets how shared mailbox access functions. Once a District email account is deactivated, access to shared mailboxes tied to that account is automatically revoked. While some departments manage mailbox permissions, these permissions cannot persist once the underlying District account is disabled.

7. Contractors

The draft does not distinguish between IT contractors, who are centrally managed with established controls, and contractors engaged by departments under separate agreements. IT tracks, monitors, and offboards its own contracted employees. By contrast, most other contractors are independent and perform their services without requiring access to District systems. Where contractors did have access, such as ActiveNet, permissions were limited to specific functions, and Finance supplements this with annual audits to confirm inactive accounts are removed.

Chicago Park District – Draft Offboarding Audit Management Response (continued)

8. Termination Dates in Section IV(C)

The report's emphasis on termination dates may give an inflated sense of risk. Even after excluding seasonal employees and duplicates, the focus on the 674 remaining employees conflates reporting lag with actual access risk. Most had only low-risk, informational email accounts, and the majority did not have ActiveNet accounts. Of the few who did, Finance was already engaged in monitoring access through the termination reporting process.

As previously confirmed with IT Applications, the weekly termination report reflects updates made in Oracle, meaning separated employees can reappear if fields are later corrected (for example, a rehire designation). This reporting mechanic helps explain the apparent over-representation of late-appearing "Do Not Rehire" employees. For employees with access to sensitive enterprise systems, HR coordinated directly with IT to ensure access was cut off promptly. For these reasons, the date of appearance on a termination report is not a reliable indicator of timeliness of access revocation.



The mission of the Office of Inspector General (OIG) is to:

- Investigate allegations of fraud, waste and abuse or misconduct by Chicago Park District employees, Board members, contractors, agents, or volunteers
- Monitor the Park District's compliance with the Employment Plan's rules governing hiring and other employment actions
- Conduct audits to enhance the effectiveness and efficiency of the District, ensure compliance with legal requirements, policies, and best practices, and mitigate risks which could impair the mission of the District.

It is the duty of every employee, Board member, agent, and contractor of the District to report any fraud, mismanagement, waste of funds or resources, abuse of authority, conflicts of interest, ethical violations or other improper act by another involving District business or assets. The Park District Code prohibits retaliation for reporting to, cooperating with, or assisting the Inspector General.

Submit a report to the Office of Inspector General through one of the following options:

- Online: <https://chicagoparkdistrict.i-sight.com/external/case/new>
- By telephone: (312) 742-3333 (Confidential Hotline)
- By fax: (312) 742-9505
- In writing: Chicago Park District Office of Inspector General, 740 N. Sedgwick St., Suite 300, Chicago, IL 60654
- In person: 740 N. Sedgwick St., Suite 300, Chicago, IL 60654