CLERK & COMPTROLLER

PALM BEACH COUNTY

AUDIT OF ACCESS REVOCATION FOR SEPARATED EMPLOYEES

SHARON R. BOCK
Clerk & Comptroller
Palm Beach County

Division of Inspector General

Audit Services Unit

March 20, 2015

SHARON R. BOCK
Clerk & Comptroller
Palm Beach County

March 20, 2015

The Honorable Sharon R. Bock, Esq.
Clerk & Comptroller

We conducted an audit to determine the timeliness and effectiveness of the Clerk & Comptroller's Office efforts to remove system access and physical access rights from employees who separate employment with the Clerk's office.

The objectives of this audit were to evaluate the processes related to eliminating system access and physical access capabilities for employees who separated from the Clerk's office and to verify such access was removed timely and accurately. Testing was also performed to determine whether revocation of access rights to the Driver and Vehicle Information Database (DAVID) complied with the Clerk's Memorandum of Understanding (MOU) with the Florida Department of Highway Safety & Motor Vehicles (DHSMV).

Our audit was neither designed nor intended to be a detailed study of every process, procedure, transaction or system in each area. Accordingly, the observations and recommendations included in this report are not all-inclusive.

We concluded that the processes in place for removing system access for separated employees are generally well-designed and effectively implemented. Exceptions were noted in deleting Active Directory accounts for former permanent and temporary employees, volunteers, and contractors. Our testing disclosed that access rights to DAVID were revoked timely and in full compliance with the Clerk's MOU with the Florida DHSMV. In regard to physical access to Clerk facilities, we confirmed that employee access badges are generally deactivated timely. Opportunities exist to strengthen monitoring efforts to identify and address occasional delays when they do occur.

We appreciated the cooperation of management and staff during the course of this audit.

Respectfully submitted,

Roger Trca CIG, CPA, CIA, MBA
Inspector General
Clerk & Comptroller Office
Palm Beach County

cc: Paul Jones, Chief Information Officer
Shannon Ramsey-Chessman, Chief Operating Officer Finance
Lisa Turner, Chief Human Resources Officer

Division of Inspector General Audit Services Unit
301 N. Olive Avenue
9th Floor
West Palm Beach, FL 33401

Phone: 561-355-2722
Fax: 561-355-7050

www.mypalmbeachclerk.com

Executive Summary

The Division of Inspector General performed an audit to determine the timeliness and effectiveness of the Clerk & Comptroller's Office efforts to remove system access and physical access rights from employees who separate from employment with the Clerk's office. This audit was added to our annual plan based on management input.

The objectives of this audit were to evaluate the processes related to eliminating system access and physical access capabilities for employees who separated from the Clerk's office and to verify such access was removed timely and accurately for a sample of prior employees. Testing was also performed to determine whether revocation of access rights to the Driver and Vehicle Information Database (DAVID) complied with the Clerk's Memorandum of Understanding (MOU) with the Florida Department of Highway Safety & Motor Vehicles (DHSMV).

We concluded that the processes in place for removing system access for separated employees are generally well-designed and effectively implemented. Periodic monitoring of access rights is in place to provide additional assurance that system access is revoked for separated employees. Exceptions were noted in deleting Active Directory accounts for former permanent and temporary employees, volunteers, and contractors. Opportunities exist to strengthen related monitoring practices for these Active Directory accounts to ensure timely deletion.

Our testing disclosed that access rights to DAVID were revoked timely and in full compliance with the Clerk's MOU with the Florida DHSMV.

In regard to physical access to Clerk facilities, we confirmed that separation notifications are transmitted to the County's Electronic Services & Security Division (ESS) and employee access badges are generally deactivated timely. However, there is no feedback or monitoring within the Clerk's office to identify occasional delays when they do occur. Additionally, timely return of access badges of separated employees was not consistently enforced and monitored prior to 2015; completion of the Employment Separation Checklist and submission to Clerk's Human Resources (HR) was made mandatory on January 15, 2015 and is expected to address this issue.

This report contains three observations and eight recommendations.

Table of Contents

Introduction **3**

Overall Conclusion 3

Objectives, Scope and Methodology 3

Background 4

Observations & Recommendations **6**

1. Active Directory security administration requires strengthening 6
2. Revocation of separated employees' access to Clerk's facilities can be enhanced. 9
3. Separation checklist communication requirements result in duplicate IT Help Desk work orders 12

Introduction

Overall Conclusion

The Clerk & Comptroller's office has a generally effective methodology in place to ensure system and application access of separated employees is disabled and deleted timely. In addition, the Clerk's office has a periodic monitoring process that provides additional assurance that access rights to various systems and applications (e.g., court operations systems, mainframe access, and PeopleSoft) are reviewed and revised as needed, including revocation of access for separated employees. The process relies upon timely feedback from management when changes are required.

The Clerk's office fully complies with the Clerk's MOU with the Florida DHSMV regarding the timeliness standard for revoking separated employee access to DAVID. Opportunities exist to strengthen Active Directory account maintenance and monitoring practices to ensure timely deletion. Revocation of physical access rights and return of access badges for separated Clerk employees should be more closely monitored.

Objectives, Scope and Methodology

The Division of Inspector General performed an audit to determine the timeliness and effectiveness of the Clerk & Comptroller's office efforts to remove system access and physical access rights from employees who separate employment. This audit of system access revocation was added to our annual plan based on management input. During the planning process, we expanded the scope to include revocation of physical access to Clerk facilities.

The objectives of this audit were as follows:

- Evaluate the processes in place related to eliminating system access and physical access capabilities for employees who have terminated employment (voluntarily or involuntarily) from the Clerk's office.
- Perform testing of a sample of employees who have terminated employment (voluntarily or involuntarily) from the Clerk's office to verify that access capabilities to select systems and applications and physical badge access to Clerk facilities were removed timely and accurately. Testing was also performed to

determine whether revocation of access rights to DAVID complied with the Clerk's MOU with the Florida DHSMV.

Our scope included analysis of the system access revocations for the 310 former employees who separated Clerk employment between January 1, 2013 and January 13, 2015. We obtained listings of these former employees from Clerk's HR.

In order to meet these objectives, we reviewed the processes related to system access and physical badge access as well revocation of these access capabilities. We interviewed HR staff involved in separation actions for Clerk employees, IT staff responsible for system access controls, and the security coordinators in IT and the Clerk's office. We evaluated the results of prior IT audits of the Clerk's office conducted by external consultants and reviewed relevant audit reports of other governmental organizations. We reviewed industry practice guides regarding the granting, maintenance, and revocation of system access rights. We performed other procedures that were deemed necessary in the circumstances. This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

Background

Clerk & Comptroller employees are granted access rights to systems and applications, which are limited to the specific functions required to perform their assigned responsibilities. Upon separation, the employee's management initiates the process guided by an Employment Separation Checklist. The checklist requires notification to HR of the pending (or immediate) separation. HR promptly transmits a Separation Notification via email to a broad distribution list (including Clerk IT, Clerk Facilities Security, and County ESS), which serves as the trigger for revocation of system access and physical access privileges.

Clerk's IT prepares a multi-step work order to guide removal of access to Clerk and County systems. The work order is assigned to Help Desk staff for execution and is tracked within the BMC FootPrints system (since August 2014), which retains information about receipt, assignment, and completion of the tasks involved. Requests received prior to August 2014 were tracked in BMC Service Desk Express, which remains available for inquiry into status and processing of work orders submitted under this prior system.

In addition, the Clerk's IT security coordinator conducts periodic reviews of system access capabilities by running access reports to Clerk's systems and applications and communicating results to Clerk managers. The objective is to verify that access rights have been revoked for separated employees and the level of access privileges granted to employees are appropriate. The periodic inquiries by IT and responses by departmental managers are maintained and the actions taken are annotated on spreadsheets.

With respect to physical access to Clerk facilities, new employees are issued either ID badges (without encoded access privileges) or access badges, depending on the requirements of their work location. Badges are issued and activated through cooperation between Clerk's HR and Clerk's Facilities Security as well as County ESS staff. Upon separation, the employee's access badge is surrendered to their manager (or Chief Officer) and forwarded to the Clerk's Facilities Security Coordinator, who records the badge in a spreadsheet and forwards badges monthly to County ESS for final revocation. The Clerk's Facilities Security Coordinator and County ESS are included on the Separation Notifications sent by HR so that badges can be deactivated and returned.

Audit Team:
Michael Bodle, Senior Internal Auditor

Observations & Recommendations

The audit identified certain policies, procedures and practices that could be improved. The audit was neither designed nor intended to be a detailed study of every relevant system, procedure or transaction. Accordingly, the observations and recommendations presented in this report may not be all-inclusive of areas where improvement may be needed.

1. Active Directory security administration requires strengthening.

Active Directory accounts provide access to the network and certain other applications. Clerk's IT disables Active Directory accounts on the effective separation date based on HR's notification. Former employee accounts are annotated by Clerk's IT indicating their accounts should be deleted 90 days after their separation date. Delays in disabling accounts increase the risk of system intrusion and unauthorized access to Clerk networks, systems and data.

Clerk's IT performs a system routine each month that identifies Active Directory accounts for which the most recent user log on is more than 90 days old to identify potential accounts for closure. This routine includes individuals who have previously logged on. Accounts with no log on activity would not be identified as an anomaly. As a result, we noted one user account for a prospective employee, who never reported to work, was not shown as an anomaly although the active account was created in 2010. Additionally, contractors and vendors are not included in this system routine for review and potential deletion.

As of December 23, 2014, there were a total of 1,008 Active Directory accounts, of which 790 accounts were assigned to individual users. Our review of the 790 individual user accounts identified 68 accounts that were not included on the active Clerk employee listing, as detailed below.

- Three permanent employees separated between six and twenty four months prior to our review. One employee separated in May 2014. Two of the separated permanent employees were former Chief Information Officers, one of whom separated from Clerk employment in January 2013 and the other separated in June 2014. According to IT, the former CIOs' accounts had been retained longer than the routine 90 days after separation to ensure the Clerk & Comptroller could receive, review, and process email traffic that may be related to Clerk business.

- Four volunteers were most recently active in 2012 and prior.
- Three temporary employees identified as interns were employed more than two years ago. One of these temporary employees had been listed as obsolete during a review in 2008.
- Also, 44 of the 68 accounts not on the active employment list were contractors or vendor employees. Clerk's IT stated they are dependent on managers for whom those contractors/vendors worked to notify IT of accounts that should be deactivated. No formal notification system is in place for departmental managers to inform IT when accounts should be disabled or deleted, and IT does not identify accounts with any recent activity for possible closure.

We examined prior reviews of Clerk IT operations performed by contracted consultants. We noted that retention of individual user accounts in Active Directory was reported as an observation in both the 2008 IT Risk Analysis Review and the 2010 IT Intrusion Security Review. In the 2008 review, the consultant identified 20 individual user accounts considered obsolete. In the 2010 review, the consultant identified 39 accounts deemed obsolete.

The remaining 218 Active Directory accounts (1,008 total less 790 individual users) were not assigned to individual users. While these accounts were not included in our audit, it appears they were largely assigned to server and training accounts. Some of the associated risks may include that these accounts are: shared among several users (thereby eliminating audit trails of system access and activity), not disabled timely, or inadequately password restricted. Adequate monitoring procedures and controls over shared Active Directory accounts are essential.

Recommendations:

A. Delete any obsolete accounts identified in Active Directory.

B. Enhance periodic review of other Active Directory accounts (e.g., contractors, vendors, volunteers and temporary employees) by including such accounts in IT's system routine and notification process for identifying, disabling and deleting these accounts.

C. Enhance IT's monthly routine used to identify inactive accounts by ensuring it flags any individual user account with no activity within the previous 90 days, rather than comparing dates of last log on.

D. Improve procedures for security administration for non-employee Active Directory accounts, particularly for temporary or short term user accounts. Consider automatically disabling such accounts unless reactivated by departmental manager within a reasonable timeframe (e.g., 90-180 days). Consider adding information in the account that identifies the department or employee responsible for disabling or reactivating the account.

E. Formalize IT procedures describing the exceptional circumstances under which an individual employee account will be kept active for more than 90 days after separation and a maximum timeframe for account retention in such cases.

Management Responses:

Information Technology management concurred with the recommendations and provided the following responses:

A. We used the user list generated during the audit review to manually locate and delete the identified stale user accounts from the Clerk Active Directory on March 13, 2015.
Target Completion Date: Completed

B. A newly updated and automated monthly routine looks for accounts in Active Directory that have never been used or have not been used in more than 90 days and generates a help desk incident listing the accounts as stale for further action, such as deletion or a written justification to remain in place. This new monthly routine has been implemented as of March 18, 2015.
Target Completion Date: Completed

C. Refer to the response in B. above for the actions taken.
Target Completion Date: Completed

D. The FootPrints Help Desk software has an updated new user creation routine with instructions to configure temporary and volunteer accounts to automatically expire after 60 days.
Target Completion Date: Completed

E. Exceptional circumstances are defined as those accounts that have highly important email accounts. We have defined a new process with County Information Systems Services (ISS) so that when an important account is deleted in Active Directory, we can ensure that new email is still delivered. County ISS performs a validity check for all incoming email by verifying the recipient is an active user in the Clerk

environment. This routine is the root cause as to why former employee email would stop being received after the account was disabled. We can continue to receive former employee email after disabling or deleting the user account by assigning the email address to existing, active resources.
Target Completion Date: Completed

2. Revocation of separated employees' access to Clerk's facilities can be enhanced.

Clerk employees are issued either ID badges or access badges upon employment, depending on the requirements of the locations that they must access to perform their duties. Badges are issued, replaced, activated, and ultimately deactivated and collected upon separation through cooperation between the Clerk's HR, Clerk's Facilities Security and County ESS staff. When employees are hired, HR notifies the Facilities Security Coordinator who arranges with County ESS to have appropriate badges issued and activated. Upon separation, the Facilities Security Coordinator and County ESS are included on an HR Separation Notification so badges can be deactivated and returned.

We selected a sample of 10 employees that had separated employment from July 1, 2014 through December 12, 2014 to review the badge deactivation and collection processes. We forwarded their names to County ESS to verify the dates on which their badges were deactivated. Of the ten separated employees:

- Two employees were issued only ID badges that do not require deactivation by County ESS.
- Five employees were deactivated within one work day and one employee within two work days of separation.
- One employee was deactivated after five work days.
- One employee was deactivated after eighteen work days.

We noted that neither HR nor the Clerk's Facilities Security Coordinator request or receive confirmation from County ESS that badges have been deactivated. We also noted that County ESS staff and the mailbox designated by ESS for the notifications had been deleted from HR's Separation Notification email distribution. After discussing this with HR and IT staff, the designated mailbox (FDO-ACCESS-Support) was re-added to the distribution list.

HR-Recruiting created a spreadsheet for Clerk's Facilities Security Coordinator to manage the badges issued and returned, and HR-HRIS (Human Resource Information Services) provides a quarterly report identifying the employees who separated, their prior work locations, and their separation dates. The Clerk's Facilities Security Coordinator enters the badge return receipt date. Our review of the spreadsheet for the 52 employee separations from September 2014 through January 2015 identified that:

- 39 separations included notations that badges were returned, with eight received more one week after separation,
- 3 separations included an annotation that the badge was not returned, and
- 10 separations had no annotation for badge return.

We were informed that badges were not always returned timely. As an example, we observed that one badge was returned on February 5, 2015 for an employee who separated May 16, 2014.

Recommendations:

A. Implement a more proactive approach for monitoring badge deactivation for separated employees, particularly for involuntary separations, and following up on the return of employee badges. For example, consideration should be given to having the Facilities Security Coordinator:
   - follow up or request confirmation from County ESS to ensure that access badges have been deactivated timely.
   - follow up with the employee's manager or contact HR if badges have not been returned timely.

B. Ensure that proposed/requested changes to the Separation Notification distribution list are routed through HR for approval prior to implementation.

Management Responses:

A. Finance management believed that the purpose of the spreadsheet referred to in the observation was to notify HR that a badge was not returned. Further, it was our understanding that no annotation, or an annotation that the badge was not returned, was notification to HR that the Facilities Security Coordinator had not received the employee's badge. County ESS has agreed to notify the Facilities Security Coordinator as soon as they deactivate an access badge. The Facilities Security Coordinator will continue to note if a badge was returned on the spreadsheet referred to above and will

begin to also note when he received confirmation from ESS that a badge was deactivated. If the Facilities Security Coordinator has not received confirmation from ESS that a badge was deactivated by the second day after separation, he will contact ESS to ensure its deactivation. If, by the second day after separation, the Facilities Security Coordinator has not received an employee's badge, or confirmation that the badge was collected and being delivered to him, he will contact the ex-employee's manager or HR to determine if it was collected. If the badge was not collected, the Facilities Security Coordinator will send a certified letter to the separated employee requesting its return.
Target Completion Date: Completed

HR management provided following additional information.

> The Facilities Security Coordinator is the designated badge recipient and should ensure badge is received timely and returned to ESS. Upon receipt of the System Notification of Separation, ESS should immediately deactivate badges, especially for involuntary terminations to minimize safety/security breach risk. HR is not responsible for requesting the badges from the managers; they are instructed to return the badge to the Facilities Security Coordinator per the Employment Separation Checklist. Based on each termination, there may be circumstances where we do not get badges returned. Certain employees are not likely to mail back their badge (e.g., resign over the phone, do not return from leave, walk off the job, terminated over the phone). If the Facilities Security Coordinator does not receive the badge (to check it off of the badge spreadsheet) in a reasonable amount of time, HR can attempt final retrieval by writing a letter to the "separated" employee, but it is not cost effective for us to pursue an inactivated badge.

B. HR management stated that changes to the Separation Notification Distribution List must be approved by a Chief Officer in writing. IT Help Desk will generate a "ticket" when making changes to the list as they maintain those lists.

Clerk IT developed a procedure documenting that a Help Desk ticket must be created to make a change to the HR notification distribution list and it must be approved by the Chief Officer of the employee's department, the Chief Operating Office of Finance, and the Chief Human Resources Officer.
Target Completion Date: Completed

3. Separation checklist communication requirements result in duplicate IT Help Desk work orders.

The Employment Separation Checklist is an HR form provided to assist departmental managers and HR staff in completing all required tasks upon an employee's separation. Since January 15, 2015, it is now mandatory that departmental managers complete itemized tasks and then forward the checklist to HR for their completion of final tasks. The checklist is used as a monitoring control by HR as well as a reminder for departmental managers.

In conducting our audit of system access revocation, we reviewed the IT BMC Service Desk Express tracking data from January 1, 2013 through August 8, 2014. During that period, we noted 21 instances in which there were duplicate requests to the Help Desk for removal of employee system access. It appears that these duplications resulted from managers acting on the checklist's instructions to notify IT to revoke employee system access as well as HR providing a Separation Notification to IT. We noted that 20 of 21 such instances involved involuntary terminations.

Departmental managers contacting Clerk's IT and HR providing a Separation Notification to IT may seem to provide an additional measure of assurance, though the cost of IT processing duplicate requests may offset the benefit. Now that the Employee Separation Checklist must be submitted to HR, departmental managers may be more consistently notifying IT and the volume of duplicated requests submitted to the IT Help Desk may rise.

Recommendation:

A. Consider revising the Employment Separation Checklist by omitting the requirement to "ensure login and password are disabled" (thereby relying upon HR's Separation Notification to IT) or by clarifying the requirement is limited to stand-alone applications that may be in use in the department.

Management Response:

A. HR stated that as of February 13, 2015, the form was modified to remove IT HelpDesk notification. There is no redundancy or duplication of IT notifications. The Employment Separation Checklist specific line item is regarding notification to "vendors" and their access as stated:

- ✓ Notify appropriate vendors that individual is no longer employed; ensure login and password are disabled.

HR management revised the checklist to clarify that this task referred to ensuring that the "vendor" login and password are disabled.

Target Completion Date: Completed