Cobb County...Expect the Best!

INTERNAL AUDIT DEPARTMENT

Report Number: 2021-004

FINAL REPORT – Review of Terminated Employees User Access Controls

August 26, 2021

Latona Thomas, CPA, Director
Erica Brooks Peters, CPA, Senior Internal Auditor
Tenaye Francois-Arneson, CIA, CFE, Senior Internal Auditor
Margarite Benevento, Senior Internal Auditor

Table of Contents

COBB COUNTY INTERNAL AUDIT

Latona Thomas, CPA
Director

100 Cherokee Street, Suite 250
Marietta, Georgia 30090
phone: (770) 528-2556
latona.thomas@cobbcounty.org

August 26, 2021

MEMORANDUM

TO: Dr. Jackie McMorris, County Manager

FROM: Latona Thomas, CPA, Director

SUBJECT: **FINAL REPORT** – Review of Terminated Employees User Access Controls

Attached for your review and comments is the subject final audit report. The overall objective of this review was to ensure that former employees do not have access to Cobb County (County) systems or data. Specifically, we evaluated the removal of user access upon the separation of service for employees to ensure the timely removal of system access privileges.

Impact on the Governance of Cobb County

The recommendations, when implemented, will strengthen the controls over terminated employee user access. County leadership and citizens can be assured that system and user access for former employees are removed in a timely manner.

Executive Summary

We determined that IS has a formal process in place to disable user access for terminated employees; however, the process is not consistently followed by all departments and improvements are needed to strengthen the current controls to ensure that access is terminated immediately and that former employees do not have access to Cobb County systems and data. Specifically, we initially identified terminated employees with system access and/or whose access was not removed timely. Additional procedures and analyses revealed that the user access for terminated employees had subsequently been disabled, the employees had been rehired, or the access was identified as an active contractor.

Recommendations

We made five (5) recommendations to strengthen the internal control environment over terminated employees' user access and to increase the completeness and accuracy of associated reports. The five recommendations are documented in the 'Results of Review' section, on Pages 4 – 9.

Responses

The Information Services Director provided a response to our draft report and concurred with all five recommendations, inclusive of one with an acceptable alternative solution. The complete responses to the draft report are included in Appendix VI. Information Services has initiated the referenced corrective actions, with an expected completion date of December 31, 2021. We will perform a follow-up on corrective action in one year from the date of this report. A copy of this report will be distributed to those affected by the report recommendations, as reflected by the distribution list in Appendix IV. Please contact me at (770) 528-2559 if you have questions.

Background

On March 18, 2020, the County transitioned to a "limited operational" status requiring that many employees shift to teleworking[1] on short notice. This transition was in response to the State of Georgia (State) Public Health State of Emergency[2] due to the impact of the coronavirus pandemic. Organizations of all sizes around the world faced a similar transition to remote work for their employees. Remote access[3] for County employees is granted via VPN[3]; must be authorized by the respective Agency, Department or Elected Official management; and granted by the Information Services (IS) Department. In addition, a telework agreement must be signed by both the employee and manager, and all equipment used in teleworking is the responsibility of the teleworker[3]. The County may not provide service or maintain any equipment needed for teleworking. If personal equipment is used for teleworking, it must be configured to comply with the County's Information Technology Policy and Security Standards and meet the minimum requirements for accessing County systems and be approved by the County. Warranty and maintenance issues are the responsibility of the teleworker.

With an increase in remote access due the coronavirus pandemic, a lack of controls around the timely termination of user access has become an emerging risk across all industries. As such, we initiated this limited scoped project to ensure that system access for County employees who separate from service is terminated timely.

Roles and Responsibilities

Human Resources Department

The Human Resources (HR) Department is responsible for processing the paperwork associated with employee terminations. In connection with the completion of any post-employment HR or Payroll related responsibilities, the termination is entered in the HR Advantage[3] system after the payroll run following the employee's last day. Terminations in the HR Advantage system are then used by IS to deprovision user access[3]. HR also distributes email notifications to various County functions. Effective October 2020, IS is also included on the email distribution list.

The remaining of this page was left blank intentionally.

[1] The practice of allowing employees to work from home, a satellite office, or other remote work centers, rather than at an employee's standard work site.

[2] The State of Georgia Executive Order No. 03.14.20.01.

[3] See Appendix II Abbreviations and Glossary.

Information Services

Information Services (IS) is responsible for the provisioning[3] and deprovisioning[3] of user access privileges. The user access is disabled for terminated employees when IS is notified in three primary ways:

- Bi-Weekly Report

  Each week, the IS Analyst that supports HR generates a report of the employees terminated from HR Advantage. Every other week, the reports are compiled and submitted to the IS Data Center Operations. The IS Data Center Operations saves the file in the IS Terminated Employees folder and creates a ticket which is made available to the Data and Telecommunications team and Server Administration team. The Data and Telecommunications team disables the phones and VPN access (if activated) and the Server Administrator disables access to Active Directory[3]. The IS Server Administration team also obtains the report, validates the employee IDs of the individuals on the report, and runs a script[3] in Active Directory to disable access for the former employees.

- Call Center /Disabling Access Form

  Department representatives from the Agency/Department or Elected Official offices submit the 'Disable Active Directory' request form (BOSS form) to notify IS of the employee terminations and request that access be disabled. This request form is submitted as an IS call center ticket. The IS Technical Operations Division or Server Administration team then uploads the termination to a spreadsheet and runs a script in Active Directory to disable access for the former employees. Section 5.9.4 in the IS Technology User Account Standards indicates that IS will disable access rights upon notification of termination of employment unless otherwise directed by the IS Director.

- Email/Phone Call

  Department representatives from the Agency/Department or Elected Official offices may also directly notify the IS Technical Operations Division or Server Administration team via email or phone call of the employee terminations and request that access be disabled. This request is converted to a call center ticket, uploaded to a spreadsheet, and the IS Technical Operations Division or Server Administration team runs a script in Active Directory to disable access for the former employee.

Agencies/Departments/Elected Official Offices

Department representatives are responsible for notifying HR and IS of terminating employees immediately upon receipt of a separation notice or as soon as the information is made available.

Primary Reports Used in the Review

1. **HR Report of Terminated Employees** - HR provided a report of employees terminated between 04/01/2020 and 9/30/2020 which was used as the population of terminated employees for testing. *Source: HR Advantage System.*

Primary Reports Used in the Review, continued

2. **Weekly Terminated Employees Report** - A script is run manually in HR Advantage to identify terminated employees. This is the source report for the Bi-Weekly Terminated Employees report. This report was used to validate the completeness of the data received from HR and the IS Technical Operations Division. *Source: IS Application Support Analyst.*
3. **Bi-Weekly Terminated Employee Report** - This report was used in the initial review of comparing to the HR Report and identifying the users with access that was disabled and the date disabled. *Source: IS Technical Operations Division.*
4. **Active Directory All Users Report** - This report captured all users for Active Directory and whether they are enabled or disabled as of 01/19/2021. This report also captured the date access was disabled for a majority of the terminated users for the project scope period. *Source: IS Technical Operations Division.*

This limited scope project covered employee terminations for the period April 1, 2020 through September 30, 2020. Detailed information on our objective, scope and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix III.

The remaining of this page was left blank intentionally.

Results of Review

Our overall objective was to ensure that former employees do not have access to Cobb County (County) systems or data. Specifically, we evaluated the removal of user access upon separation from service for employees to ensure the timely removal of system access privileges. The preliminary survey was performed concurrently with the fieldwork phase. The steps involved information gathering, data validation, detailed testing, and the evaluation of results. We also conducted numerous interviews with HR and IS to identify the process involved to disable access for terminated employees. Data validation and analyses included comparing the weekly termination reports generated by the IS Application Support Analyst to the bi-weekly report used by the IS Technical Operations Division and the HR report of terminations. The reports were all generated from the HR Advantage system, either directly or indirectly. Due to the initial discrepancies found, additional manual procedures were performed. Based on our testing, we determined that IS has a formal process in place to disable user access for terminated employees. This process includes the use of the Disable Active Directory request form, the use of a bi-weekly report from HR, and a validation of the employee ID numbers to ensure the accuracy of the user access accounts disabled. However, the process is not consistently followed by all departments and improvements are needed to strengthen the current controls to ensure that access is terminated immediately and that former employees do not have access to Cobb County systems and data. Specifically, we initially identified former employees with access to the Active Directory and/or terminated employees that were not removed immediately. The accompanying pages include several recommendations to address and strengthen the County's internal control environment over terminated employees' user access.

Control Activities in the Terminated Employee User Access Process Need Improvement

During the period 4/1/2020 and 9/30/2020, we identified 337 employees on the HR report of terminated employees, including three (3) that transferred from full to part-time and are still employed at the County. With the remaining 334 employees, we analyzed various reports used to disable system access to identify the population of users disabled during the scope period. Using the HR and IS reports received, we analyzed and identified the timeframe between the employee's separation from service and the date disabled by the IS Technical Operations Division Server Administration team. Our analysis also included 31 manual requests to disable user access made directly to IS. We observed terminated employees whose Active Directory account had not been disabled; terminated employees whose access had not been terminated timely; employees with no system access; and an inconsistent method used to request that terminated employee access be disabled. Other improvements include additional validation controls and the use of consistent report parameters.

After our initial analysis, we identified a list of terminated employees for which we were unable to confirm access had been disabled. We discussed the initial results with the IS Technical Operations Division and subsequently obtained a report of all users as of 01/19/2021. Using a series of additional automated and manual procedures and analysis, we identified the status (i.e. enabled or disabled) of each terminated employee's user access per this report.

Of our population of 334 terminated employees, we noted that 214 user access had been disabled, 56 were still enabled, and another 64 were potentially identified as seasonal and may have never had access to the system. See Table 1 to the right. The next three sections include further details into each status.

Status of Terminated Employees	
Disabled	214
Enabled	56
Not on Active Directory (No system access)	64
Total	334

Table 1 – Source: IS and HR Reports.

User Access Enabled for Terminated Employees

As referenced previously, we observed that the user access for 56 terminated employees was still enabled per an active directory account report dated as of 1/19/2021. HR confirmed that six employees have been rehired in a full-time or part-time capacity. One additional user access is due to a special request to leave the user access enabled to ensure that necessary emails could be obtained following this employee's departure. Of the remaining 49 former employees, we noted that nine were captured on the bi-weekly reports to be disabled but were not disabled. The remaining 40 had not been captured during the bi-weekly process and included one June 2020 report that was not properly transferred between IS teams. We were unable to determine why the user access for these 49 terminated employees had not been disabled, but we performed additional procedures to obtain the current status. We obtained an active directory account report on June 30, 2021, and noted that 47 of the 49 former employees had subsequently been disabled. The remaining two are active contractors.

The user access for terminated employees should be disabled immediately upon departure from the County. The internal process to disable access is dependent upon the transfer of termination reports between IS teams; however, it does not include a validation or review of the results to ensure user access was disabled as expected. Therefore, former employees may have access to County systems or data or may have access for several days or weeks following their respective termination dates, which could result in improper changes or destruction of data, programs, or files.

Terminated Employees user access is not disabled timely

The user access for terminated employees is not disabled immediately upon departure from the County in all instances. We reviewed the account status of 334 terminated employees for the period under review and confirmed that 214 terminated employee user accounts had been properly disabled, but 89% or 190 of those had not been disabled timely[4]. Eight of which were manual direct requests to IS to disable access after the employee's date of termination. We also noted one (1) special request to leave the account open so that email could be accessed for work in progress. Chart 1 to the right represents the number of days to disable user access for the 214 terminated employee user accounts disabled.

Number of Accounts Disabled and the Number of Days to Disable

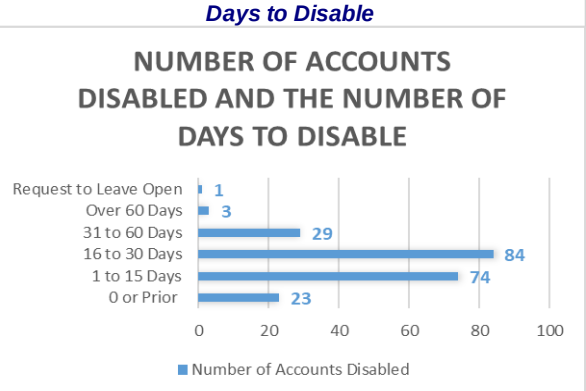

Chart 1 - Source: IS and HR Reports.

[4] Not timely represents accounts disabled one or more days after a terminated employee separates from service.

Because the current process to disable user access relies primarily upon the HR Advantage bi-weekly report, it can take several days or weeks beyond an employee's termination date for their access to be disabled. As such, the employee's name would not appear on the HR report until after any payroll or other HR related activities specific for that employee's termination are complete. Former employees could have access to County systems or data for several days or weeks following their termination date, resulting in improper changes or the destruction of data, programs or files.

Employees with No System Access

We also noted that 64 were not found on the Active Directory All User Access report. Upon review of their roles per the HR report, we determined that 57 did not have access to Active Directory due to the nature of their positions (i.e. 53 seasonal and four per diem). We were unable to determine the specific reason the remaining seven employees did not have access, but IS staff believes these were the result of removing employee accounts after 90 days. IS previously deleted terminated employee accounts over 90 days but subsequently discontinued that process. Though unable to verify the specifics, we were able to determine that these employees did not have system access as of 01/19/21 per the Active Directory All User Access report.

Inconsistent Method Used to Request that User Access be Disabled

The method used to request that user access be disabled for terminated employees is not consistent across the County. Accounts are disabled using a bi-weekly report from HR Advantage; the use of the 'Disable Active Directory Account Request' form on iCOBB; or direct request via emails or phone calls. The Technology Acceptable Use Standards references the County form and location to request the disabling of an employee's active directory account; however, the use of this form is not consistently required to disable user access. Industry best practices also require a consistent process to deprovision user access of terminated employees. Due to the timing of termination and the procedures required to be performed by HR upon an employee's departure, the employee may not be captured on the bi-weekly report to disable access until several days or weeks after their termination date. In addition, we identified user access privileges for some former employees that have not been disabled. Former employees may still have access to County systems or data or have access for several days or weeks following their respective termination dates, resulting in improper changes or the destruction of data, programs, or files.

Additional Validation Controls are Needed

There is no validation to confirm that terminated employee user access is disabled for the bi-weekly report of terminated employees. As part of the bi-weekly process to disable access for terminated employees, an IS server administrator reviews the employee ID per the bi-weekly report and confirms that the employee ID matches the employee ID in Active Directory. The bi-weekly report of terminated employees is then used to disable user access within Active Directory; however, there is no subsequent validation to ensure that the user access was disabled as expected for the employees on the report. Of the 56 terminated employees whose access had not been disabled, our testing identified nine out of 14 that were included on the bi-weekly reports to disable access but not disabled, with the other five having resumed employment with the County. See 'User Access Enabled for Terminated Employees' section on Page 5 for further discussion.

A review of the results should be performed by the IS server administrator (and/or manager) to confirm access has been disabled as expected. The current process of terminating employee user access does not include a documented review of the results to ensure user access was disabled as expected. Former employees may have access to County systems or data resulting in improper changes or the destruction of data, programs, or files.

Effective monitoring controls over user access terminations are essential to ensure that user access is terminated as intended and in a consistent manner. Management reviews at the functional or activity level is a basic internal control activity which compares actual performance to planned or expected results. This activity must be ongoing to ensure expected management objectives and goals are met. These activities include approvals, authorizations, verifications, reconciliations, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation.

Recommendations

The Information Services Director or Designee should:

Recommendation 1: Require the 'Disable Active Directory Account' form as the primary control to disable employee user access. The form should be submitted in advance of the employee's termination date, if known and not later than the termination date if not known in advance.

***Auditee Response*:** **Concur with Alternate Solution.**

As a result of the Terminated Employees User Access audit, IS and HR has developed a new Employee Termination Process. The process starts with HR being notified of someone leaving. HR fills out a spreadsheet with FirstName, LastName, EmployeeID, Department, Unit and Date of Termination (DOT) plus some other HR specific information. Daily at 5:40 PM the spreadsheet is picked up and processed by an automated script that sends the spreadsheet to the HR Terminations Distribution Group and processes the people in the list. If the person's DOT is today or in the past the account is disabled. If the DOT is in the future, the account is set to expire/disable on that date. Records of all transactions are recorded and saved in log files. If a match is not found a ticket is open and it is looked at by a member of the server admin team.

Based on this new workflow, we have found that the Boss form is redundant and causes issues within the workflow. We have more than a few employees that leave and come back as a contractor or volunteer almost immediately. The Boss form is not always handled the same day or in the order they were intended so accounts get disabled when they should be converted to Contractor/Volunteer accounts. By eliminating the Boss form for employee terminations there is no longer redundant reporting and processes are not being done out of order.

The Boss form is also used incorrectly when someone transfers departments. The Department that is losing the employee asks that the employee be removed from all systems. Since this comes in the Termination ticket and not a transfer, the employee is disabled. By no longer using the form for employee terminations this will no longer happen. The form should still be used for non-Employees.

IS Management will re-evaluate the forms to develop a more clear separation of purpose.

Recommendation 2: Formally document the expectations around the requirement to notify and timing of notification to IS of terminating employees. The form should be submitted in advance of the employee's termination date, if known in advance.

***Auditee Response*: Concur**

When it is determined that an employee will no longer work for Cobb County Government the Departments should notify HR that day. If an employee leaves abruptly the Department should contact the Call Center immediately and notify them of the situation so the employee's account can be disabled. The Department should then follow the standard HR procedures. IS is in the process of updating the Information Technology Policy and associated standards documents, including the Technology User Account Standards. Once this review and update is complete it will be part of an annual countywide IS policy review and approvals for all employees that will occur in January. We will also work with HR, HR Department Reps, Department Heads, and other Department personnel on additional education on these procedures.

Recommendation 3: Coordinate with HR to ensure that additional countywide education on the requirement is distributed to all County agencies, departments, and elected official offices.

***Auditee Response*: Concur**

IS is in the process of updating the Information Technology Policy and associated standards documents, including the Technology User Account Standards. Once this review and update is complete it will be part of the annual countywide policy review and approvals for all employees that will occur in January. We will also work with HR, HR Department Reps, Department Heads, and other Department personnel on additional education on these procedures.

Recommendation 4: Disable user access immediately upon the employee's departure.

***Auditee Response*: Concur**

As a result of the Terminated Employees User Access audit, IS and HR has developed a new Employee Termination Process. The process starts with HR being notified of someone leaving. HR fills out a spreadsheet with FirstName, LastName, EmployeeID, Department, Unit and Date of Termination (DOT) plus some other HR specific information. Daily at 5:40 PM the spreadsheet is picked up and processed by an automated script that sends the spreadsheet to the HRTerminations Distribution Group and processes the people in the list. If the person's DOT is today or in the past the account is disabled. If the DOT is in the future, the account is set to expire/disable on that date. Records of all transactions are recorded and saved in log files. If a match is not found a ticket is open and it is looked at by a member of the server admin team.

The remaining of this page was left blank intentionally.

Use of Consistent Report Parameters Needed

We noted discrepancies between the weekly report generated by the IS Application Support Analyst, the HR report of terminated employees and the bi-weekly report used by IS Technical Operations Division. We obtained and attempted to validate various employee termination reports for completeness and accuracy. We had planned to analyze the revised results and assess our ability to rely on our source population of terminated employees before proceeding with our audit procedures. We noted inconsistencies and thus had to conduct additional interviews, perform additional procedures, analyses, and reconciliations; and perform numerous manual processes to obtain a sufficient level of assurance in order to rely on the information received.

The parameters used to generate reports of terminated employees from the HR Advantage system should be consistent, periodically reviewed, and/or updated to ensure that the population used to terminate user access is complete and accurate. Discrepancies between the reports could indicate the data is inaccurate or incomplete and therefore, lead to former employees with access to County systems or data, resulting in improper changes or the destruction of data, programs, or files.

Recommendation

The Information Services Director or Designee should:

Recommendation 5: Coordinate with Human Resources and perform a review of the parameters used to generate the reports to ensure that the data used in disabling user access is accurate and complete. This process should be performed periodically on an ongoing basis.

***Auditee Response*: Concur**

IS Management and HR Management will review the parameters used to generate the reports on a semi-annual basis.

Appendix I

Detailed Objective, Scope, and Methodology

We conducted this limited scope audit in accordance with The Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing. The overall objective was to ensure that former employees do not have access to Cobb County (County) systems or data. We evaluated the removal of user access upon the separation of service for employees to ensure the timely removal of system access privileges. The limited scope project covered employees that were terminated between 04/01/2020-9/30/2020.

Data validation procedures were performed on the reports obtained. For the report of terminated employees provided by HR and the reports provided by IS, we reviewed the report parameters to confirm that the report captured the data requested. The weekly generated report from HR Advantage (i.e. source report) for the bi-weekly reports was obtained and compiled to compare to the bi-weekly reports from the IS Technical Operations Division and the report of terminations from HR, with discrepancies as noted in the results section.

I. Determined if the controls in place are adequate to ensure the removal of user access for all terminated employees is timely.

   A. Interviewed the HR Specialist to gain an understanding of HR's role in termination of employee user access process.

   B. Interviewed the IS Division Director or designee to gain an understanding of IS's role in the termination of employee user access process.

   C. Reviewed the IS policies and standards to evaluate whether they address the requirements for removing user access for terminated employees.

   D. Obtained an HR report of the employees that were terminated between 04/01/2020 and 9/30/2020 along with the separation of service dates and a report from IS detailing disabled Active Directory user accounts between 04/01/2020 and the date requested. Testing was performed to validate the timeliness and completeness of terminated employee user access.

   E. Obtained a report of IS call center tickets between 4/1/2020 and 09/30/2020 entered directly by the IS Call Center team to identify the Agency, Department or Elected Official direct requests to IS to remove employee access to County applications in advance of the HR process. Testing was performed to ensure that employee user access to County systems are timely removed as requested.

Appendix II

Abbreviations and Glossary

Abbreviations

HR	Human Resources Department
IS	Information Services Department
VPN	Virtual Private Network
DOT	Date of Termination

Glossary

User Access - also called user rights, the authorization given to users that enables them to access specific resources on the organization's network, such as data files, applications and so forth.

Provisioning - involves the security process of granting and updating access of an individual user to an organization's resources.

Deprovisioning – involves the security process of removing access for an individual user to an organization's resources.

Remote Access – the technology and techniques used to give authorized user access to an organization's networks and systems from off-site. The action or practice of working from home making use of the internet, email and the telephone.

VPN – Type of security mechanism that extends a private network across a public network and enables users to send and receive data across a shared or public network as if their computing devices were directly connected to the private network. It primarily provides an additional layer of authentication and security.

Active Directory – A database and set of services that connect users with network resources and enables administrators to manage user permissions and control access to network resources.

Script – A list of commands that are executed by a certain program or scripting engine. Scripts may be used to automate processes.

HR Advantage – The system used for the input and maintenance of HR related data, including employee information such as start and termination dates.

Teleworker – An employee that is permitted to work from their home, or other suitable location, and he or she will be responsible for adhering to the guidelines of the Teleworking Policy which includes working at least the number of hours that will be paid for that day. A Teleworker's job may require that all or part of a teleworking day be forfeited due to the priorities in the office. This priority will be determined by the Telemanager.

Telemanager – A manager that directly supervises the Teleworker. The Telemanager is responsible for evaluating the effectiveness of the program for each participant. If a problem arises that cannot be resolved, the Telemanager is responsible for termination of the teleworking agreement.

Appendix III

Major Contributors to This Report

Latona Thomas, CPA, Internal Audit Director
Erica Brooks Peters, CPA, Auditor-in-Charge
Tenaye Francois-Arneson, CFE, CIA, Senior Internal Auditor

Appendix IV

Final Report Distribution List

Jimmy Gisi, Deputy County Manager
Sharon Stanley, Support Services Agency Director
Kimberly Lemley, Information Services Director
Ed Biggs, Information Services Technical Operations Division Director
John Harwood, Technology Services Manager
Tony Hagler, Human Resources Director
Cobb County Audit Committee
Internal Audit Department File

Appendix V

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on County governance. These benefits will be incorporated into our annual report to the Board of Commissioners, Audit Committee, and County Manager.

Type and Value of Outcome Measure:

- Increased Safeguards over County Systems and Data– Actual; Recommendations, when implemented, will provide increased controls over County systems and data. (See Pages 4 - 9).
- Compliance with County Policy – Actual; Recommendation, when implemented, will provide assurance that a consistent use of the 'Disable Active Directory Account Request' form is used to ensure that terminated employee's user access is disabled timely. (See Pages 6 - 8).
- Reliability of Information – Actual; Recommendations, when implemented, will provide assurance on the overall data reliability, as well as the completeness and accuracy of terminated user access reports. (See Pages 6 - 9).

Methodology Used to Measure the Reported Benefit:

For the period 04/01/2020-9/30/2020, we identified 337 employees on the HR report of terminated employees, including three (3) that transferred from full to part-time and are still employed at the County. We analyzed various HR and IS reports and identified the timeframe between the employee's separation from service and the date disabled.

Appendix VI

Auditee's Response to the Draft Report

COBB COUNTY
INFORMATION SERVICES DEPARTMENT
Kimberly B. Lemley
Information Services Director
100 Cherokee Street, Suite 520
Marietta, Georgia 30090-7000
770.528.8700 • fax: 770.528.8706
Kimberly.Lemley@cobbcounty.org

DATE: August 17, 2021

TO: Latona Thomas, CPA, Director, Internal Audit

FROM: Kimberly B. Lemley, Director, Information Services

SUBJECT: Audit Response - Review of Terminated Employees User Access Controls

Several recommendations were made and our response to those recommendations are below

Recommendation 1: Require the 'Disable Active Directory Account' form as the primary control to disable employee user access. The form should be submitted in advance of the employee's termination date, if known and not later than the termination date if not known in advance.

Response: Concur with Alternate Solution

As a result of the Terminated Employees User Access audit, IS and HR has developed a new Employee Termination Process. The process starts with HR being notified of someone leaving. HR fills out a spreadsheet with FirstName, LastName, EmployeeID, Department, Unit and Date of Termination (DOT) plus some other HR specific information. Daily at 5:40 PM the spreadsheet is picked up and processed by an automated script that sends the spreadsheet to the HRTerminations Distribution Group and processes the people in the list. If the person's DOT is today or in the past the account is disabled. If the DOT is in the future, the account is set to expire/disable on that date. Records of all transactions are recorded and saved in log files. If a match is not found a ticket is open and it is looked at by a member of the server admin team.

Based on this new workflow, we have found that the Boss form is redundant and causes issues within the workflow. We have more than a few employees that leave and come back as a contractor or volunteer almost immediately. The Boss form is not always handled the same day or in the order they were intended so accounts get disabled when they should be converted to Contractor/Volunteer accounts. By eliminating the Boss form for employee terminations there is no longer redundant reporting and processes are not being done out of order.

The Boss form is also used incorrectly when someone transfers departments. The Department that is losing the employee asks that the employee be removed from all systems. Since this comes in the Termination ticket and not a transfer, the employee is disabled. By no longer using the form for employee terminations this will no longer happen. The form should still be used for non-Employees.

IS Management will re-evaluate the forms to develop a more clear separation of purpose.

Recommendation 2: Formally document the expectations around the requirement to notify and timing of notification to IS of terminating employees. The form should be submitted in advance of the employee's termination date, if known in advance.

Response: Concur

When it is determined that an employee will no longer work for Cobb County Government the Departments should notify HR that day. If an employee leaves abruptly the Department should contact the Call Center immediately and notify them of the situation so the employee's account can be disabled. The Department should then follow the standard HR procedures. IS is in the process of updating the Information Technology Policy and associated standards documents, including the Technology User Account Standards. Once this review and update is complete it will be part of an annual countywide IS policy review and approvals for all employees that will occur in January. We will also work with HR, HR Department Reps, Department Heads, and other Department personnel on additional education on these procedures.

Recommendation 3: Coordinate with HR to ensure that additional countywide education on the requirement is distributed to all County agencies, departments and elected official offices.

Response: Concur

IS is in the process of updating the Information Technology Policy and associated standards documents, including the Technology User Account Standards. Once this review and update is complete it will be part of the annual countywide policy review and approvals for all employees that will occur in January. We will also work with HR, HR Department Reps, Department Heads, and other Department personnel on additional education on these procedures.

Recommendation 4: Disable user access immediately upon the employee's departure.

Response: Concur

As a result of the Terminated Employees User Access audit, IS and HR has developed a new Employee Termination Process. The process starts with HR being notified of someone leaving. HR fills out a spreadsheet with FirstName, LastName, EmployeeID, Department, Unit and Date of Termination (DOT) plus some other HR specific information. Daily at 5:40 PM the spreadsheet is picked up and processed by an automated script that sends the spreadsheet to the HRTerminations Distribution Group and processes the people in the list. If the person's DOT is today or in the past the account is disabled. If the DOT is in the future, the account is set to expire/disable on that date. Records of all transactions are recorded and saved in log files. If a match is not found a ticket is open and it is looked at by a member of the server admin team.

Recommendation 5: Coordinate with Human Resources and perform a review of the parameters used to generate the reports to ensure that the data used in disabling user access is accurate and complete. This process should be performed periodically on an ongoing basis.

Response: Concur

IS Management and HR Management will review the parameters used to generate the reports on a semi-annual basis.