Miami-Dade County Public Schools

Internal Audit Report

Audit of LEGACY/SAP Systems: Security Controls, Roles, And Access Management In Reference To Charter Schools And District Vendors/Contractors

System Modifications, Updates To Certain Documents, And User Training Would Improve System Security And Enhance Controls Over Access To Personally Identifiable Information (PII).

JULY 2020

THE SCHOOL BOARD OF MIAMI-DADE COUNTY, FLORIDA
Ms. Perla Tabares Hantman, Chair
Dr. Steve Gallon III, Vice Chair
Dr. Dorothy Bendross-Mindingall
Ms. Susie V. Castillo
Dr. Lawrence S. Feldman
Dr. Martin Karp
Dr. Lubby Navarro
Dr. Marta Pérez
Ms. Mari Tere Rojas

Superintendent of Schools
Mr. Alberto M. Carvalho

Office of Management and Compliance Audits
Ms. Maria T. Gonzalez, CPA
Chief Auditor

Contributors to This Report:

Audit Performed by:
Mr. Luis O. Baluja, CISA
Mr. Neil R. Singh, CPA
Ms. Patricia Tumelty, MBA

Audit Supervised by:
Mr. Jon Goodman, CPA, CFE

Audit Reviewed by:
Mr. Luis O. Baluja, CISA
Mr. Jon Goodman, CPA, CFE

Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools
Alberto M. Carvalho

Chief Auditor
Maria T. Gonzalez, CPA

Miami-Dade County School Board
Perla Tabares Hantman, Chair
Dr. Steve Gallon III, Vice Chair
Dr. Dorothy Bendross-Mindingall
Susie V. Castillo
Dr. Lawrence S. Feldman
Dr. Martin Karp
Dr. Lubby Navarro
Dr. Marta Pérez
Mari Tere Rojas

June 26, 2020

The Honorable Chair and Members of The School Board of Miami-Dade County, Florida
Members of The School Board Audit and Budget Advisory Committee (ABAC)
Mr. Alberto M. Carvalho, Superintendent of Schools

Ladies and Gentlemen:

We have performed an audit of the LEGACY/SAP Systems: Security Controls, Roles, and Access Management in accordance with the approved 2019-2020 Fiscal Year Audit Plan. The objective of this audit was to assess the internal controls for granting and managing access to the LEGACY and SAP systems for Charter Schools and District vendors/contractors.

This is the second audit related to SAP and LEGACY controls. The first audit, presented to the ABAC at its September 17, 2019, meeting focused on traditional schools and District offices.

This audit resulted in five findings identifying the need for improvement over the monitoring and reconciliation of user access, reducing exposure of Personally Identifiable Information (PII), a need for training, and greater awareness of security policies and best practices. The audit also offers corresponding recommendations and management responses.

We would like to thank the management of Information Technology Services, Charter Schools Compliance and Support, and District offices that participated in this audit for their cooperation and courtesies extended to our staff.

Sincerely,

Maria T. Gonzalez

Maria T. Gonzalez, CPA
Chief Auditor
Office of Management and Compliance Audits

TABLE OF CONTENTS

Page
Number

TABLE OF CONTENTS (CONTINUED)

Page
Number

EXECUTIVE SUMMARY

Information Technology Services (ITS) provides the technical infrastructure and foundation that supports the District's instructional, operational, and business processes. ITS provides access to the LEGACY and SAP systems (***S****ystems,* ***A****pplications, and* ***P****roducts*) via a primarily decentralized authorization process. This process is generally governed by the District's Network Security Standards (NSS) document which was last updated in August of 2017.

The objective of this audit was to assess the internal controls for granting and managing access to the LEGACY and SAP systems to Charter Schools and District vendors/contractors and to review procedures for periodic monitoring and reconciliation of user access.

The audit resulted in five findings and corresponding recommendations as follows:

- In our sample testing of 15 Charter Schools, a number of LEGACY authorizations issued to Charter School employees were determined to be excessive because they were inappropriate based upon position, role, or the user's assigned responsibilities; and this excess should be eliminated to safeguard information and prevent the system from potential inappropriate use. This was in contrast with SAP authorizations, where access was limited to the Principal. Charter School Principals interviewed were either unaware of a required monthly reconciliation policy to maintain control over the issuance of LEGACY authorizations or were not familiar as to how to perform this procedure. A similar finding was discussed with District Administration during our Audit of LEGACY/SAP Systems, published by our office in September 2019, and corrective actions were implemented to address those prior conditions. Regarding this audit and going forward, the District's Office of Charter Schools Compliance and Support, in collaboration with the Charter Schools, should monitor and enforce monthly compliance with the reconciliation policy requirement and provide training to all Charter School Principals on how to perform the review.

- During our testing, we identified a certain LEGACY subsystem which poses a potential risk of exposing sensitive information. This concern was discussed with management and the details of the finding have been omitted for security purposes.

- In nine out of 15 Charter Schools sampled (60%), Principals were unable to provide evidence that their school had adopted a computer and privacy policy, pursuant to contract. Further, Charter School employees do not receive periodic reminders related to accessing District systems, such as an acknowledgement, requesting their confirmation and acceptance of the District's access policies. We recommend that Charter Schools Compliance and Support and the appropriate Charter School Governing Boards, enforce the contractual requirements with the District regarding the formal adoption of a computer and privacy policy. Additionally, ITS should explore the implementation of a system-generated acknowledgement of District systems policies, at least annually, for Charter School employees as is currently implemented for District employees.

- The current SAP Security Roles Report and the LEGACY reconciliation report are not complete in regard to vendor information and Charter School employee job/title descriptions. This prevents Charter School Principals and Site Administrators from properly monitoring and reconciling Charter employee and Contractor access to these systems. We recommend that ITS review the SAP and LEGACY reconciliation report-generation process and programming to ensure that accurate information is provided to Charter School and District Site Administrators.

- Displaying a System Use Notification message prior to accessing District systems places the user on notice that unauthorized access to the information contained therein may subject the user to civil and/or criminal penalties. This message would serve as a deterrent and support enforceability actions in the event of inappropriate access. We recommend that the District consider placing a System Use Notification message prior to accessing any District system, including LEGACY and SAP.

Management's responses to the findings and recommendations are included on pages 9 through 15 following each individual finding, and in memorandum format as received by our office starting on page 17. We have also included a glossary of technical terms and acronyms on page 16.

INTERNAL CONTROLS

Our overall evaluation of internal controls over the delegation and monitoring of access to the LEGACY/SAP systems by Charter Schools and vendors is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls		✓	
Policy & Procedures Compliance		✓	
Effect		✓	
Information Risk		✓	
External Risk		✓	

INTERNAL CONTROLS LEGEND			
CRITERIA	SATISFACTORY	NEEDS IMPROVEMENT	INADEQUATE
Process Controls	Effective	Opportunities exist to improve effectiveness	Do not exist or are not reliable
Policy & Procedures Compliance	In compliance	Non-compliance issues exist	Non-compliance issues are pervasive, significant, or have severe consequences
Effect	Not likely to impact operations or program outcomes	Impact on outcomes contained	Negative impact on outcomes
Information Risk	Information systems reviewed are secure and accurate	Information systems reviewed are mostly secure and accurate but can be improved	Information systems reviewed are not secure or accurate and can result in data exposure or negatively affect decision making
External Risk	None or low	Potential for damage	Severe risk of damage

BACKGROUND

Miami-Dade County Public Schools (referred to as the "District") relies on networked devices and data processing facilities to store and process critical data and Personally Identifiable Information (PII) such as student, personnel, business, and accounting records. Granting access to this data is accomplished via a primarily decentralized[1] authorization process whereby ITS grants Site Administrators the ability to delegate access to users under their supervision as they deem appropriate. The Site Administrator is usually the most senior person at a location such as the School Principal or Department Head.

The LEGACY system, commonly known as the *Customer Information Control System* (CICS), is gradually being phased out. Existing subsystems within LEGACY are being migrated to new platforms, including *Systems, Applications, and Products* (SAP). LEGACY currently serves as the System of Record (SOR) for student academic, attendance, and personal information. Pursuant to contractual requirements between the District and Charter Schools, all Charter School student information must be posted to the LEGACY system. In addition, Charter School personnel information is also housed within LEGACY.

SAP is the vendor that developed the Enterprise Resource Planning (ERP) system in use by the District. SAP currently houses and processes financial, business, and personnel information, including the District's payroll. At the time of this audit, Charter School employees have minimal access to SAP. Certain vendors/contractors may require access to both the LEGACY and SAP systems, dependent upon their duties and the needs of the contracting work location.

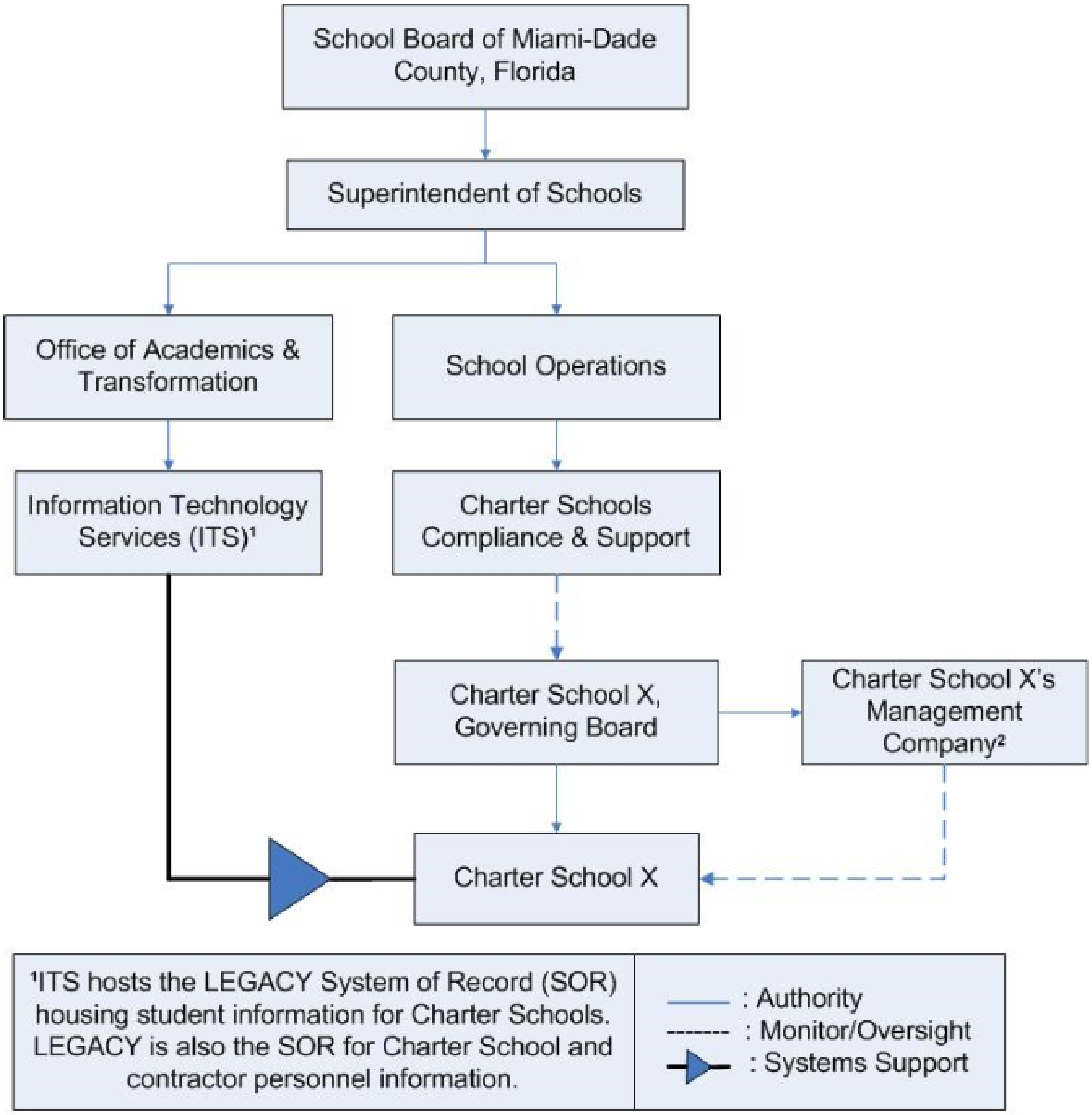
Every month, a LEGACY *Resource Access Control Facility* (RACF) report is generated by ITS and an *SAP Security Roles* report can be generated on demand by the Site Administrator. Both reports are used to review systems authorizations held by users under the Site Administrator's purview.

Site Administrators are required to print, review, make changes to user access as necessary, date and sign both reports every month, and archive 12 months of reviewed reports for audit purposes. The objective is to document the periodic review of user access, ensure that any previous changes were accurately processed, and that the authorizations held by staff are appropriate.

An organizational chart, as it relates to the scope of this audit, is presented on the following pages for both Charter Schools and District vendors/contractors.

[1] The District's Office of Charter Schools Compliance and Support and various "owner" departments also facilitate this process for Charter Schools and vendors/contractors, respectively.

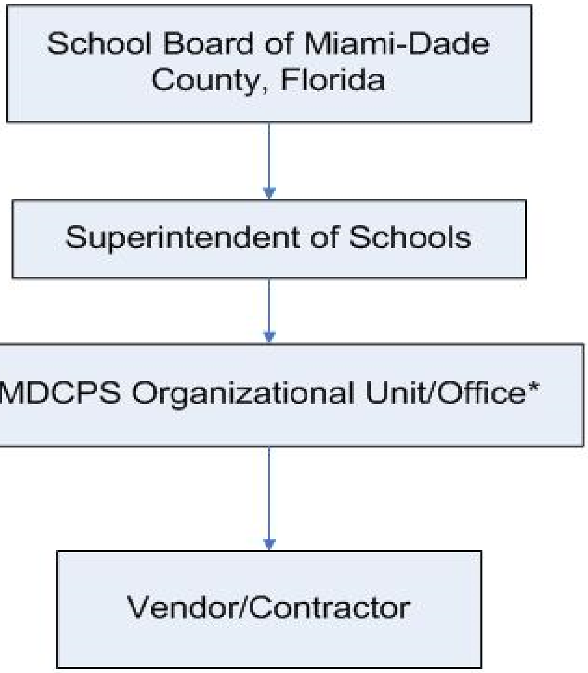
Charter Schools - Organizational Chart


School Board of Miami-Dade County, Florida
Superintendent of Schools
Office of Academics & Transformation
School Operations
Information Technology Services (ITS)[1]
Charter Schools Compliance & Support
Charter School X, Governing Board
Charter School X's Management Company[2]
Charter School X
: Authority
------- : Monitor/Oversight
: Systems Support

[1] ITS hosts the LEGACY System of Record (SOR) housing student information for Charter Schools. LEGACY is also the SOR for Charter School and contractor personnel information.

[2] A majority, but not all, of Charter Schools Operating in Miami-Dade County have contracted with a management company.

Contractors - Organizational Chart



School Board of Miami-Dade County, Florida

Superintendent of Schools

MDCPS Organizational Unit/Office*

Vendor/Contractor

* The “owner” of the contracted services is typically the office, Department, or Work Location paying for the service.

OBJECTIVES, SCOPE AND METHODOLOGY

We performed this audit in accordance with the approved 2019-2020 Fiscal Year Audit Plan. The objectives were to assess the internal controls for managing and provisioning user access, review procedures for periodic monitoring and reconciliation of access, and ensure that the organization complies with generally accepted standards, laws, regulations, and internal policies that govern the user authorization process.

The scope of the audit was comprised of LEGACY and SAP authorizations for Charter School employees and District vendors/contractors as of February 2020.

We performed the following procedures to satisfy our objectives:

- Obtained an understanding of the District's relationship with Charter Schools and various vendors/contractors, as it relates to the scope of our audit;
- Interviewed vendors/contractors, Site Administrators, and staff at various Charter Schools and District offices;
- Reviewed numerous Charter School and Vendor contracts;
- Analyzed access data;
- Performed tests of user access and reviewed roles associated with the access;
- Reviewed LEGACY *Resource Access Control Facility* (RACF) reports;
- Reviewed SAP Security Roles reports;
- Reviewed prior audit findings;
- Performed site visits to test appropriateness of authorizations and internal controls;
- Observed the various access screens detailing critical information; and,
- Reviewed applicable policies, procedures, standards, and best practices:

  - ➢ M-DCPS Network Security Standards
  - ➢ Various School Board Policies
  - ➢ Various M-DCPS manuals and other publications
  - ➢ Various *Weekly Briefings*
  - ➢ National Institute of Standards and Technology (NIST) Publication 800-53r4
  - ➢ Previous work performed by other audit entities

We selected a sample and visited 15 Charter Schools (approximately 11% of the total population) based upon the various management companies servicing the schools. We also selected eight vendors/contractors (approximately 10%) based upon those vendors/contractors that had some level of access to either the LEGACY and/or SAP systems, as reported to us by ITS.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards* (GAGAS) issued by the Comptroller General of the United States of America Government Accountability Office (GAO). Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Certain details have been omitted from this report for security purposes pursuant to Section 281.301, Florida Statutes, Security systems; records and meetings exempt from public access or disclosure.

FINDINGS AND RECOMMENDATIONS

1. Opportunities Exist To Minimize Charter School Employee Authorization/Access To LEGACY Applications

From our sample of 15 Charter Schools selected for this audit, we found that all schools tested disclosed varying degrees of excessive LEGACY authorizations delegated to Charter School employees that were not required or inappropriate based upon the position, role, or the user's assigned responsibilities. Consequently, the excess of authorizations should be revoked to safeguard information and prevent the system from exposure to potentially inappropriate use of information. This was in contrast with SAP authorizations which were only being used by the Principal for the procurement of supplies.

The primary cause for issuing/allowing these many authorizations to employees is that Charter School Principals were not aware of their responsibility to reconcile user access or how to perform said reconciliations.

The policy is detailed in the District's Network Security Standards (NSS) document, which is extended to Charter Schools pursuant to their executed Charter School contracts. Site Administrators are required to review and retain a signed and dated copy of both the LEGACY RACF and SAP Security Roles reports on a monthly basis to document the review, showing any changes made, and confirming that the authorizations held by staff are appropriate. Reviewed RACF and SAP Security Roles reports are to be initialed and retained for 12 months for audit purposes.

Both the NSS and National Institute of Standards and Technology guidance state that access must be granted following the *Principle of Least Privilege* (PoLP). This concept requires granting users with the minimum amount of access needed to carry out their duties.

Charter School Principals stated that they had not been informed of the NSS policy requirement and had not received *Weekly Briefings* issued by the District reminding them of this requirement. However, as a result of a similar finding and related recommendation discussed with District Administration during our Audit of Legacy/SAP Systems that was published in September 2019, Charter School Principals received a notification via electronic mail from the District's Chief Information Security Officer titled *Reminder to Review RACF and SAP Roles Reports – January 2020* on January 28, 2020, reminding them of this requirement.

The absence of a consistent monthly monitoring process and a lack of training on how to perform said reconciliation procedure has resulted in a significant number of unneeded or inappropriate user authorizations, some of which provide access to critical or Personally Identifiable Information.

Recommendations

1.1. Charter School Principals should perform the monthly reconciliation as required by their contractual agreements with the District. The Office of Charter School Compliance and Support, in collaboration with the various Charter School Governing Boards, should monitor and enforce monthly compliance with the reconciliation requirement.

Responsible Department(s): **Applicable Charter Schools**
Charter School Compliance and Support

Management's Response:

The Office of Charter School Compliance and Support (CSCS) is in receipt of the Legacy/SAP Audit Report and is in agreement with Finding 1.1 as related to the requirements for charter school administrators to review RACF and SAP Roles on a monthly basis. In order to ensure compliance with requirements, CSCS will implement the practices described below:

Training/Professional Development - In collaboration with ITS, CSCS will facilitate modules during New Schools Training (July/August) and the annual Charter School Principals Opening of Schools Meeting (August/September) to provide a review the of District's Network Security Standards, charter school responsibilities related to the District's Network Security Standards, and the RACF and SAP Roles and Review processes required, inclusive of standards relative to the concept of granting access using the established and approved Principle of Least Principle (PoLP) concept. Participation in this training and receipt of materials will be recorded, monitored and maintained for compliance purposes. Recognizing the turnover in charter school administrators, this training module will be recorded and made available, on an as needed basis, for the on-boarding of new principals throughout the school year. As with the in-person training, participation in this virtual training will also be recorded, monitored and maintained.

Monthly Reconciliation - CSCS will utilize its on-line monitoring system wherein charter school site administrators will upload a signed and dated copy of both the LEGACY RACF and SAP Security Roles reports to document the review, showing any changes made, and confirming that the authorizations held by staff are appropriate and allowable. Reviewed RACF and SAP Security Roles reports are to be retained for audit purposes. Charter school principals will utilize this process to confirm that they have reviewed SAP access monthly to ensure that only applicable approved personnel have appropriate access and that access for those individuals whose employment and/or roles have been changed, has been terminated. Secondly, ITS will provide CSCS staff access to reconciliation reports to perform random audits or reviews, as determined.

2. Access To Sensitive Data Should Be Restricted

During our testing, we identified a certain LEGACY subsystem which poses a potential risk of exposing sensitive information.

This concern was discussed with management and the details of the finding have been omitted from this report for security purposes pursuant to Section 281.301, Florida Statutes, Security systems; records and meetings exempt from public access or disclosure.

Recommendation

2.1. ITS should update the specific subsystem to address the concern discussed with management.

Responsible Department(s): ITS

Management's Response:

The scope of the project in the referenced briefing (WB 16683) was pertaining to student systems; however, ITS acknowledges the potential concerns and will modify the identified system to mitigate exposure risks and work with other departments to limit access to that system.

3. Adoption And Acknowledgement Of The District's Systems Access Policy For Charter Schools Should Be Formally Implemented

In nine out of 15 Charter Schools sampled (60%), Principals were unable to provide evidence that the Charter School had adopted a computer and privacy policy, pursuant to contractual requirements. Further, Charter School employees do not receive periodic reminders related to accessing District systems, such as an acknowledgement, requesting their confirmation and acceptance of the District's access policies.

Following is a sample of the *Acceptable Use Policy* language found in all reviewed Charter School contracts, in pertinent part:

> *The School shall adopt student and employee computer and privacy policies and standards that comply with all applicable state and federal laws. All Charter School employees and students are bound by all of the Sponsor's computer policies and standards regarding data privacy and system security. The School shall not access, directly or through a third party, any of the Sponsor's student information unless and until the student actually enrolls in the School. Violation of this provision constitutes good cause for termination.*

The District's NSS document states, in pertinent part:

> *Acceptance of employment or contracts with M-DCPS will signify acceptance of these standards by the user. Failure to comply with this or any M-DCPS computer security policy or standard may result in termination of employment, termination of contract, and/or prosecution. Employees must annually acknowledge that they have read and understand these guidelines.*

The lack of adoption and acknowledgement of a computer and privacy policy weakens user awareness and enforceability and is not in compliance with contractual requirements.

<u>Recommendation</u>

3.1. Charter School Governing Boards and Charter School Compliance and Support should enforce the contractual requirement and adoption of a computer and privacy policy.

Responsible Department(s): **Applicable Charter Schools**
Charter School Compliance and Support

Management's Response:

CSCS is in receipt of the Legacy/SAP Audit Report and is in agreement with Finding 3.1 as related to the adoption and acknowledgement of the District's systems access policy. In order to ensure compliance with requirements, CSCS will implement the following practices:

While the charter school contract creates the mechanism to enforce charter school employees and students to comply with the District's computer policies and standards regarding data privacy and systems security, the following additional steps will be implemented to enforce this requirement and adoption of a computer and privacy policy:

1. In collaboration with ITS, written guidance regarding this contractual provision will be issued by CSCS to all charter school governing boards and school administrators, along with a copy of the District policy. Additionally, CSCS will add a page on its department website that lists charter-relevant district policies and charter school compliance responsibilities for future reference.

2. To ensure evidence of adoption of the policy as required by the charter contract, CSCS will provide each charter school governing board chairperson an attestation form to execute which will acknowledge receipt and adoption of the District's Systems Access Policy for its charter school(s). In the event the District changes its policy subsequent to initial execution, a new attestation form will be reissued to the Governing Board Chairpersons for execution to ensure transparency and knowledge of any revisions. The attestation forms will be issued, tracked, monitored, and archived for future reference.

3. During CSCS site visits and/or desk audits, various policies and practices are reviewed for compliance. The current list of policies/practices will be amended, requiring charter school site administrators to provide evidence that all staff and students have acknowledged receipt and understanding of the District's computer policies and standards regarding data privacy and system security.

4. Improvements Over Reconciliation Reports And Inclusion Of Complete Information Are Needed

Work Site Administrators are responsible for monitoring and reconciling contractor access to SAP using a feature referred to as the SAP *Security Roles Report*. This report can be generated on demand by the Site Administrator and shows SAP authorizations held by individual staff members or the entire work location.

We generated the reports by user and work location with vendors/contractors and found that for all 12 vendors/contractors tested, both reports showed that the user did not have any access to SAP, or “no assignments found for employee number X”. However, when we utilized an alternative method that is not published or known to location Site Administrators, we discovered that some vendors/contractors did in fact have significant access to various SAP authorizations, including those that allow for viewing of Personally Identifiable Information (PII).

When we reviewed the LEGACY reconciliation reports (RACF reports), we found that none of the reports were populated with the title/job description of Charter School staff. As a result, the reviewer of the report is unable to properly reconcile access based upon the role of the user.

As described in Finding #1, both system reports must be reviewed for appropriate authorizations by site supervisors on a monthly basis for employees and for other non-employees such as consultants and vendors/contractors.

In addition, the National Institute of Standards and Technology AC-5 details the importance of Separation of Duties. Dividing functions among different individuals and/or roles is critical to addressing the potential for abuse of system access and helps reduce the risk and exposure of PII. It is critical that the SAP Security Roles Report displays all authorizations held by a contractor so that the Site Administrator can properly reconcile and administer the authorizations review.

Furthermore, pursuant to the National Institute of Standards and Technology AU-3, “the information system must generate audit records containing user title, role, job description, or any other information that establishes the identity of any individuals or subjects associated with the audit records.”

Recommendations

4.1. ITS should review the SAP Security Roles report generation process and programming to ensure that all authorizations held by vendors/contractors are listed in the report.

4.2. ITS should review the RACF report generation process and programming to ensure that LEGACY reconciliation reports are populated with Charter School user job title/description.

Responsible Department(s): ITS

Management’s Response:

4.1 When the SAP Roles Report was originally developed, roles being given to vendors/contractors was not widespread. Because roles are assigned to a position rather than to the user and contractors do not have a position in SAP, the current reporting mechanism is unable to provide information for individuals who do not have a position (i.e., anyone who is a non-employee and does not appear in the “Org,” such as contractors/vendors); as such, a separate report will be developed to encompass all non-employees.

4.2 M-DCPS employee access to legacy system references data located in PERS (legacy HR application for employees); since Charter (and other non-Miami-Dade County Public Schools) employees originate in ACES rather than PERS, the user’s name and employee number are listed in the report, but the employee’s title/description information does not exist directly in the files generated by ACES and is therefore not listed on the report. ITS will investigate the possibility of leveraging position/job code located in ACES to extract the requested information from a separate file and integrate into the existing report.

5. A System Use Notification Message To Support Appropriate Use And Enforceability Of Unauthorized Access Should Be Implemented

Currently, a warning or other message about inappropriate access to the LEGACY and SAP systems is not in place.

As described in the National Institute of Standards and Technology AC-8, a system access and use notification message, prior to accessing the LEGACY or SAP systems, places the user on notice that unauthorized access or use of the information contained therein may subject the user to civil and/or criminal penalties. The System Use Notification message serves as a deterrent and supports enforceability actions in the event of inappropriate access.

Recommendation

5.1 A System Use Notification message should be implemented prior to users accessing the LEGACY or SAP systems. Ideally, such a message would be placed prior to portal login, making the message applicable to nearly all systems accessible to users.

Responsible Department: ITS

Management's Response:

ITS acknowledges the potential benefits of this type of warning and will investigate the feasibility of inserting a disclaimer at the Portal login prompt. It should be noted that finding 5 was not changed to an Observation as requested. While management's response does concur with and plans to implement the recommendation, it does not agree with a best practice being the basis of an audit finding. Again, we respectfully request that this finding be modified to an observation.

Auditor's Comment:

We are pleased that the Administration agrees with this recommendation (and all five of our other recommendations herein) to further improve security and access controls relative to charter schools and vendors/contractors. Regarding the Administration's request to downgrade this finding to an "observation", we maintain that it is a finding as Section 8.124 of *Government Auditing Standards* (2018 Revision) specifies that criteria for a finding may include "laws, regulations, contracts, grant agreements, **standards**, measures, expected performance, **defined business practices**, and benchmarks against which performance is compared or evaluated". In this finding, both standards and business practices apply as the finding's criteria.

GLOSSARY OF TECHNICAL TERMS/ACRONYMS

The following definitions are provided for abbreviations and acronyms used in this report:

CICS	**Customer Information Control System -** LEGACY system
ITS	**Information Technology Services -** Central District IT facility
NIST	**National Institute of Standards and Technology** – A national organization charged with developing Information Technology security standards and guidelines for governmental information systems
NSS	**Network Security Standards** – Delineates security guidelines for M-DCPS
PII	**Personally Identifiable Information -** Defined as information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name)
PoLP	**Principle of Least Privilege** - Generally accepted standard of providing systems access based on need
RACF	**Resource Access Control Facility** - Provides LEGACY access and controls
SAP	**Systems, Applications, and Products**
SOR	**System of Record**
WB	**Weekly Briefings -** the District's centralized information distribution tool

APPENDIX

MANAGEMENT'S RESPONSE MEMORANDUM

MEMORANDUM **June 19, 2020**

TO: Maria T. Gonzalez, Chief Auditor
Office of Management and Compliance Audits

FROM: Jaime G. Torrens, Chief of Staff
Office of the Superintendent

SUBJECT: REVISED DRAFT REPORT - AUDIT OF LEGACY/SAP SYSTEMS: SECURITY CONTROLS, ROLES AND ACCESS MANAGEMENT IN REFERENCE TO CHARTER SCHOOLS AND DISTRICT VENDORS/CONTRACTORS

In response to the revised draft report - Audit of Legacy/SAP Systems: Security Controls, Roles and Access Management in Reference to Charter Schools and District Vendors and Contractors, below are management's responses:

Finding 1: Opportunities Exist To Minimize Charter School Employee Authorization/Access To LEGACY Applications

Recommendation:

1.1. Charter School Principals should perform the monthly reconciliation as required by their contractual agreements with the District. The Office of Charter School Compliance and Support, in collaboration with the various Charter School Governing Boards, should monitor and enforce monthly compliance with the reconciliation requirement.

Management's Response:

The Office of Charter School Compliance and Support (CSCS) is in receipt of the Legacy/SAP Audit Report and is in agreement with Finding 1.1 as related to the requirements for charter school administrators to review RACF and SAP Roles on a monthly basis. In order to ensure compliance with requirements, CSCS will implement the practices described below:

> Training/Professional Development - In collaboration with ITS, CSCS will facilitate modules during New Schools Training (July/August) and the annual Charter School Principals Opening of Schools Meeting (August/September) to provide a review the of District's Network Security Standards, charter school responsibilities related to the District's Network Security Standards, and the RACF and SAP Roles and Review processes required, inclusive of standards relative to the concept of granting access using the established and approved Principle of Least Principle (PoLP) concept. Participation in this training and receipt of materials will be recorded, monitored and maintained for compliance purposes. Recognizing the turnover in charter school administrators, this training module will be recorded and made available, on an as needed basis, for the on-boarding of new principals

throughout the school year. As with the in-person training, participation in this virtual training will also be recorded, monitored and maintained.

Monthly Reconciliation - CSCS will utilize its on-line monitoring system wherein charter school site administrators will upload a signed and dated copy of both the LEGACY RACF and SAP Security Roles reports to document the review, showing any changes made, and confirming that the authorizations held by staff are appropriate and allowable. Reviewed RACF and SAP Security Roles reports are to be retained for audit purposes. Charter school principals will utilize this process to confirm that they have reviewed SAP access monthly to ensure that only applicable approved personnel have appropriate access and that access for those individuals whose employment and/or roles have been changed, has been terminated. Secondly, ITS will provide CSCS staff access to reconciliation reports to perform random audits or reviews, as determined. -

Finding 2. Access to sensitive data should be restricted

Recommendation:

2.1. ITS should update the specific subsystem to address the concern discussed with management.

Management's Response:

The scope of the project in the referenced briefing (WB 16683) was pertaining to student systems; however, ITS acknowledges the potential concerns and will modify the identified system to mitigate exposure risks and work with other departments to limit access to that system.

Finding 3. Adoption and acknowledgement of the District's Systems Access Policy for Charter Schools should be formally implemented

Recommendation:

3.1. Charter School Governing Boards and Charter School Compliance and Support should enforce the contractual requirement and adoption of a computer and privacy policy.

Management's Response:

CSCS is in receipt of the Legacy/SAP Audit Report and is in agreement with Finding 3.1 as related to the adoption and acknowledgement of the District's systems access policy. In order to ensure compliance with requirements, CSCS will implement the following practices:

While the charter school contract creates the mechanism to enforce charter school employees and students to comply with the District's computer policies and standards regarding data privacy and systems security, the following additional steps will be implemented to enforce this requirement and adoption of a computer and privacy policy:

1. In collaboration with ITS, written guidance regarding this contractual provision will be issued by CSCS to all charter school governing boards and school administrators, along with a copy of the District policy. Additionally, CSCS will add a page on its department website that lists charter-relevant district policies and charter school compliance responsibilities for future reference.

2. To ensure evidence of adoption of the policy as required by the charter contract, CSCS will provide each charter school governing board chairperson an attestation form to execute which will acknowledge receipt and adoption of the District's Systems Access Policy for its charter school(s). In the event the District changes its policy subsequent to initial execution, a new attestation form will be reissued to the Governing Board Chairpersons for execution to ensure transparency and knowledge of any revisions. The attestation forms will be issued, tracked, monitored, and archived for future reference.

3. During CSCS site visits and/or desk audits, various policies and practices are reviewed for compliance. The current list of policies/practices will be amended, requiring charter school site administrators to provide evidence that all staff and students have acknowledged receipt and understanding of the District's computer policies and standards regarding data privacy and system security.

Finding 4. **Improvements Over Reconciliation Reports And Inclusion Of Complete Information Are Needed**

Recommendations:

4.1. ITS should review the SAP Security Roles report generation process and programming to ensure that all authorizations held by vendors/contractors are listed in the report.

4.2. ITS should review the RACF report generation process and programming to ensure that LEGACY reconciliation reports are populated with Charter School user job title/description.

Management's Responses:

4.1 When the SAP Roles Report was originally developed, roles being given to vendors/contractors was not widespread. Because roles are assigned to a position rather than to the user and contractors do not have a position in SAP, the current reporting mechanism is unable to provide information for individuals who do not have a position (i.e., anyone who is a non-employee and does not appear in the "Org," such as contractors/vendors); as such, a separate report will be developed to encompass all non-employees.

4.2 M-DCPS employee access to legacy system references data located in PERS (legacy HR application for employees); since Charter (and other non-Miami-Dade County Public Schools) employees originate in ACES rather than PERS, the user's name and employee number are listed in the report, but the employee's title/description information does not exist directly in the files generated by ACES and is therefore not listed on the report. ITS will investigate the possibility of leveraging position/job code located in ACES to extract the requested information from a separate file and integrate into the existing report.

Finding 5. **The System Use Notification Message To Support Appropriate Use And Enforceability Of Unauthorized Access Should Be Implemented**

Recommendation:

5.1 A System Use Notification message should be implemented prior to users accessing the LEGACY or SAP systems. Ideally, such a message would be placed prior to portal login, making the message applicable to nearly all systems accessible to users.

Management's Response:

ITS acknowledges the potential benefits of this type of warning and will investigate the feasibility of inserting a disclaimer at the Portal login prompt. It should be noted that finding 5 was not changed to an Observation as requested. While management's response does concur with and plans to implement the recommendation, it does not agree with a best practice being the basis of an audit finding. Again, we respectfully request that this finding be modified to an observation.

If you have any questions or require additional information, or wish to schedule a briefing, please contact me at 305 995-2393 or 305 218-2705.

IRMC:ajo
M061
cc: Mr. Alberto M. Carvalho
Mrs. Valtena G. Brown
Ms. Marie L. Izquierdo
Ms. Iraida R. Mendez-Cartaya
Mr. Ron Y. Steiger

Anti-Discrimination Policy

Federal and State Laws

The School Board of Miami-Dade County, Florida adheres to a policy of nondiscrimination in employment and educational programs/activities and strives affirmatively to provide equal opportunity for all as required by:

Title VI of the Civil Rights Act of 1964 - prohibits discrimination on the basis of race, color, religion, or national origin.

Title VII of the Civil Rights Act of 1964 as amended - prohibits discrimination in employment on the basis of race, color, religion, gender, or national origin.

Title IX of the Education Amendments of 1972 - prohibits discrimination on the basis of gender.

Age Discrimination in Employment Act of 1967 (ADEA) as amended - prohibits discrimination on the basis of age with respect to individuals who are at least 40.

The Equal Pay Act of 1963 as amended - prohibits gender discrimination in payment of wages to women and men performing substantially equal work in the same establishment.

Section 504 of the Rehabilitation Act of 1973 - prohibits discrimination against the disabled.

Americans with Disabilities Act of 1990 (ADA) - prohibits discrimination against individuals with disabilities in employment, public service, public accommodations and telecommunications.

The Family and Medical Leave Act of 1993 (FMLA) - requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to "eligible" employees for certain family and medical reasons.

The Pregnancy Discrimination Act of 1978 - prohibits discrimination in employment on the basis of pregnancy, childbirth, or related medical conditions.

Florida Educational Equity Act (FEEA) - prohibits discrimination on the basis of race, gender, national origin, marital status, or handicap against a student or employee.

Florida Civil Rights Act of 1992 - secures for all individuals within the state freedom from discrimination because of race, color, religion, sex, national origin, age, handicap, or marital status.

Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA) - prohibits discrimination against employees or applicants because of genetic information.

Boy Scouts of America Equal Access Act of 2002 – no public school shall deny equal access to, or a fair opportunity for groups to meet on school premises or in school facilities before or after school hours, or discriminate against any group officially affiliated with Boy Scouts of America or any other youth or community group listed in Title 36 (as a patriotic society).

Veterans *are provided re-employment rights in accordance with P.L. 93-508 (Federal Law) and Section 295.07 (Florida Statutes), which stipulate categorical preferences for employment.*

In Addition:
School Board Policies 1362, 3362, 4362, and 5517 - Prohibit harassment and/or discrimination against students, employees, or applicants on the basis of sex, race, color, ethnic or national origin, religion, marital status, disability, genetic information, age, political beliefs, sexual orientation, gender, gender identification, social and family background, linguistic preference, pregnancy, citizenship status, and any other legally prohibited basis. Retaliation for engaging in a protected activity is also prohibited.

For additional information contact:

Office of Civil Rights Compliance (CRC)
Executive Director/Title IX Coordinator
155 N.E. 15th Street, Suite P104E
Miami, Florida 33132
Phone: (305) 995-1580 TDD: (305) 995-2400
Email: crc@dadeschools.net Website: http://crc.dadeschools.net

Rev: 08/2017

Miami-Dade County Public Schools

Internal Audit Report

Audit of LEGACY/SAP Systems: Security Controls, Roles, and Access Management In Reference To Charter Schools and District Vendors/Contractors

JULY 2020

Office of Management and Compliance Audits
1450 N. E. 2nd Avenue, Room 415
Miami, Florida 33132
Tel: (305) 995-1318 • Fax: (305) 995-1331
http://mca.dadeschools.net