Miami-Dade County Public Schools

Internal Audit Report

Audit of Legacy/SAP Systems – District-Wide Security Controls, Roles, and Access Management

Opportunities exist to improve controls over monitoring access to Legacy applications, and in adherence by site administrators, to established standards and procedures.

September 2019

Contributors to This Report:

Audit Performed by:
Mr. Neil R. Singh, CPA
Mr. Wilmer Maradiaga, MS

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

Audit Reviewed by:
Mr. Luis O. Baluja, CISA
Ms. Teresita Rodriguez, CPA

Miami-Dade County Public Schools

giving our students the world

Superintendent of Schools
Alberto M. Carvalho

September 17, 2019

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 Legacy/SAP (*Systems, Applications, and Products)* Systems – District-Wide Security Controls, Roles, and Access Management in accordance with the approved 2018-2019 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 and to review procedures for periodic monitoring and reconciliation of access by site administrators.

The scope of the audit comprised all active Legacy and SAP authorizations for all District school-sites and non-school sites as of March 2019.

The audit resulted in four findings identifying the need for improvement over the monitoring and reconciliation of user access to systems applications, and additional training of site administrators in this area. The audit also offers corresponding recommendations.

We would like to thank the management of Information Technology Services and select District management for their cooperation and courtesies extended to our staff during this audit.

Sincerely,

Maria T. Gonzalez

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

TABLE OF CONTENTS

Page
Number

FINDINGS AND RECOMMENDATIONS

APPENDIX

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 via a primarily decentralized authorization process. This process is governed by the District's Network Security Standards (NSS) 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 and to review procedures for periodic monitoring and reconciliation of user access.

The scope of this audit comprised all active Legacy and SAP authorizations for all District school sites and non-school sites as of March 2019.

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

- Approximately eight percent of Legacy authorizations tested were determined to be inappropriate to the user based upon the position, role, or the user's assigned responsibilities. This was in contrast with SAP authorizations, where the number of authorizations to be terminated was immaterial. When a potential discrepancy was identified, it was discussed with the site administrator and corrected upon their concurrence. School Operations should consider reviewing with site administrators their responsibility to perform monthly reconciliations of user authorizations in both systems to ensure that access is limited to those who require it based on their duties and responsibilities.

- A complete and accurate legend of the various types of Legacy and SAP authorizations was not readily available. The Data Security, Governance and Compliance section of ITS should ensure that the RACF Authorization and SAP Roles legends are updated and monitor/review these legends periodically to ensure that all authorizations have meaningful/understandable and accurate descriptions of their capabilities.

- From our site visits and testing, we found instances where Food Service Managers had transferred to another school or location, however, Legacy user access to the former site's information had not been revoked. The Department of Food and Nutrition should ensure that this reconciliation and removal process is performed going forward.

- In interviews conducted by OMCA staff, almost half (i.e., 10 of 21) of site administrators cited difficultly and/or unfamiliarity with the process of generating Legacy and/or SAP reconciliation reports. ITS should consider programming that would generate reconciliation reports that are automatically and predictably sent to a site administrator's email every month.

Certain details regarding location and specific user access have been omitted from this report for security reasons.

Management’s responses to the findings and recommendations are included on pages 8 through 12, following each individual finding, and in memorandum format as received by our office on pages 13 and 14.

INTERNAL CONTROLS

Our overall evaluation of internal controls over the District's process of granting and monitoring access specific to Legacy/SAP 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 are reliable	Data systems are mostly accurate but can be improved	Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions
External Risk	None or low	Potential for damage	Severe risk of damage

BACKGROUND

Miami-Dade County Public Schools relies on networked devices and data processing facilities to store and process critical 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 by means of an application referred to as *Quad A*. *Quad A* allows site administrators, instead of ITS, the ability to grant and manage systems and applications access to users under their supervision as they deem appropriate. The site administrator is usually the most senior person at that location such as the School Principal or Department Head.

The Legacy system, commonly known as the Customer Information Control System or "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 for student academic and personal information and the District's Property inventory, among others.

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 and is used to process the District's payroll.

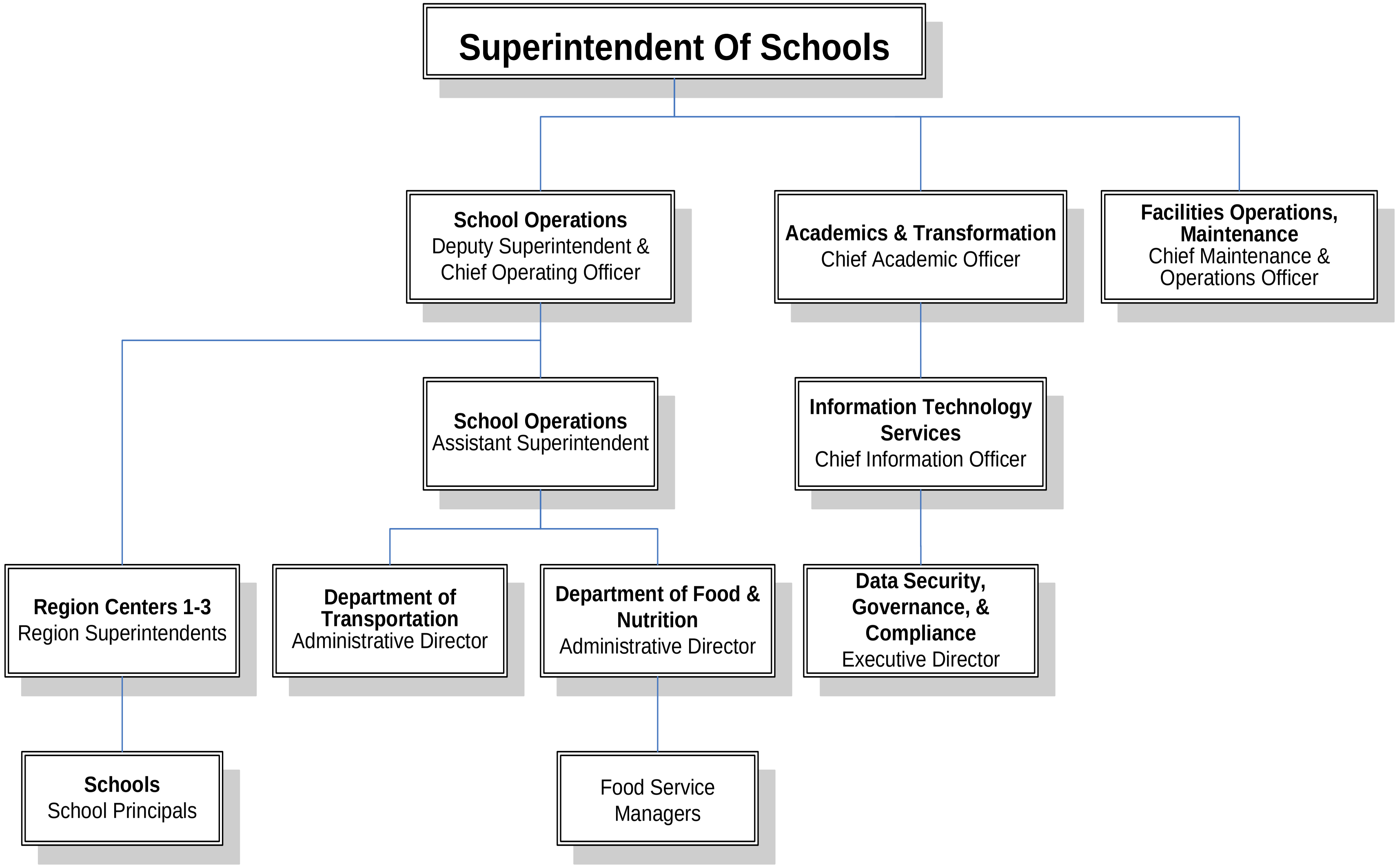
Every month, a *Legacy Resource Access Control Facility* (RACF) report is generated by ITS and an *SAP Security Roles* report can be generated on demand by the site administrator. Both reports are available to site administrators to review all systems authorizations held by users under their purview.

Site administrators are required to print, review, make changes to user access as necessary, date and sign both reports every month, and archive twelve 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.

A partial organizational chart, as it relates to the scope of this audit, is presented on the following page.

[1] Certain SAP authorizations are assigned centrally based on an employee's position.

Partial Organizational Chart



Superintendent Of Schools

School Operations
Deputy Superintendent &
Chief Operating Officer

Academics & Transformation
Chief Academic Officer

Facilities Operations, Maintenance
Chief Maintenance &
Operations Officer

School Operations
Assistant Superintendent

Information Technology Services
Chief Information Officer

Region Centers 1-3
Region Superintendents

Department of Transportation
Administrative Director

Department of Food & Nutrition
Administrative Director

Data Security, Governance, & Compliance
Executive Director

Schools
School Principals

Food Service
Managers

OBJECTIVES, SCOPE AND METHODOLOGY

We performed this audit in accordance with the approved 2018-2019 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 to 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 comprised all active Legacy and SAP authorizations for all District school sites and non-school sites as of March 2019.

Audit procedures included:

- Interviewing appropriate ITS staff;
- Interviewing site administrators and staff at various schools and District offices;
- Obtaining two databases of Legacy and SAP authorizations;
- Analyzing access data;
- Reviewing Legacy Resource Access Control Facility (RACF) reports;
- Reviewing SAP Security Roles reports;
- Reviewing applicable statutes, policies, procedures, and best practices;
- Reviewing the Legacy RACF Authorization and the SAP Roles Legends;
- Creating two “dictionaries” of Legacy and SAP authorizations;
- Reviewing prior audit findings;
- Performing site visits to test appropriateness of authorizations and review internal controls;
- Observing the various access screens detailing critical information; and,
- Reviewing forms and processes utilized in granting access.

Samples were selected judgmentally from a population of approximately 110,000 and 34,000 critical[2] Legacy and SAP authorizations, respectively. Twenty-one schools or departments were selected for site visits spanning various regions and levels (e.g. elementary, middle, senior high schools). When a potential discrepancy was identified, it was discussed with the site administrator and corrected upon their concurrence.

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 and specifics have been omitted from this report for security reasons.

[2] Prior to beginning the fieldwork for this audit, OMCA staff met with senior ITS staff and agreed on which Legacy and SAP authorizations were critical based on accessibility to Personally Identifiable Information (PII) of employees and students, and proprietary business functions.

FINDINGS AND RECOMMENDATIONS

1. Opportunities Exist To Minimize Inappropriate Authorization/Access To Legacy Applications

We found that 782 (8.3%) of 9,477 Legacy authorizations tested were determined to be inappropriate based upon the position, role, or user's assigned responsibilities and needed to be terminated. This was in contrast with SAP authorizations, where the number of authorizations to be terminated was immaterial. When a potential discrepancy was identified, it was discussed with the site administrator and corrected upon their concurrence. Inappropriate authorization could increase the risk of unauthorized access to critical business and Personally Identifiable Information (PII) of employees and students.

The determination as to whether a user's access was appropriate is based on 1) the site administrator's discretion, 2) the Principle of Least Privilege (PLP)[3], and 3) established criteria [Network Security Standards (NSS – last updated in August 2017) and policy updates].

The primary cause of inappropriate Legacy authorizations was non-adherence to the District's NSS, which requires the site administrator to reconcile authorizations via monthly Legacy RACF and SAP Security Roles reports for 12 consecutive months. Of the 21[4] sites visited, 16 site administrators (76%) were unable to provide documentation evidencing that said reconciliations had been performed for Legacy applications.

Also contributing to instances of inappropriate authorizations is that site administrators were not always familiar with NSS and policy and procedures updates that are customarily disseminated to district staff and administration via *Weekly Briefings*, the District's centralized information distribution tool.

For example, *Weekly Briefing* #19237 (published in April 2016), states that the electronic Gradebook (WGBM) and Attendance Manager (WGBA) authorizations are limited to five individuals. However, from our interviews, we determined that site administrators were not always familiar with these briefings and the associated requirements. Although the NSS is included in a package provided to school site administrators at the opening of the school year, it appears that it may be overlooked. In addition, non-school site administrators do not routinely receive the package with the NSS documentation.

[3] The "Principle of Least Privilege" is defined as a default of no access to resources and the requirement of explicit permission and authorization by the owner based on need. (MDCPS NSS, August 2017)

[4] Comprised of 13 schools and eight non-school site departments.

Recommendations

1.1. School Operations should consider reviewing with site administrators their responsibility to perform monthly reconciliations of user authorizations in both systems, the PLP, and ensuring that inappropriate user access is timely revoked.

1.2. Previously published *Weekly Briefings* with important security updates should be considered for redistribution and those that reference access to applications should be incorporated into the NSS. ITS should redistribute the NSS to site administrators and, going forward, this document should be updated and distributed as necessary.

Responsible Departments: School Operations, ITS

Management's Response:

School Operations will provide a review to site administrators through Scaled Leadership to ensure they perform monthly reconciliations of user authorization and minimize authorization/access to Legacy/SAP applications. Moving forward, weekly briefings regarding these applications and security updates will be published each year (as applicable) as a compliance feature in the School Operations Management Guide.

ITS will redistribute weekly briefings with important security updates as appropriate. The Network Security Standards will continue to be updated and distributed as necessary. Significant changes to the NSS will prompt a weekly briefing to all employees to raise awareness to changes that may have a significant impact on regular user functions.

2. The RACF Authorization And SAP Roles Legends Should Be Updated

A complete and accurate Legend of the various types of Legacy and SAP authorizations was not readily available. When requested by the OMCA, a list of approximately 800 Legacy authorizations was provided. This list was titled *"RACF Authorization Legend".* However, 91 of the authorization descriptions were missing, and 132 were labeled as not in use, obsolete, or replaced by SAP, etc. Throughout the course of the audit, ITS continuously updated both authorization legends as they obtained information from the various system owners.

ITS provided a list titled "Roles Legend" of over 22,000 SAP authorizations and identified 88 that were applicable[5] to the School District. However, 14 of the 88 authorizations that are routinely granted were missing descriptions, while other descriptions were presented in technical terms not recognizable to most site administrators. Also, some descriptions did not adequately describe the intent, resulting level of access, and abilities that would be provided to the user.

According to ITS, the Data Security, Governance and Compliance section of ITS periodically performs cataloging and monitoring of the RACF and SAP Roles legends. However, this continues to be a work in progress. Consistent with sound internal controls and generally accepted practices, a complete listing of all authorizations, together with meaningful/understandable descriptions, will allow a site administrator to properly evaluate the authorizations being delegated to staff. Similarly, complete descriptions permit site administrators to appropriately conduct monthly reviews of staff authorizations.

Recommendation

2.1. The Data Security, Governance and Compliance section of ITS should ensure that the RACF Authorization and SAP Roles Legends are updated and monitor these legends at least annually going forward to ensure that all authorizations have meaningful/understandable and accurate descriptions of their capabilities.

Further, ITS should consider programming updates that would enable site administrators to view a dropdown list of available authorizations and their related descriptions when granting access to applications.

Responsible Department: ITS

[5] Other than the 88 applicable authorizations, the remaining authorizations are default or "built-in" to SAP's foundation and not used by M-DCPS.

Management's Response:

ITS is in the process of updating the RACF Authorization and SAP Roles legends in order to provide a comprehensive and easy-to-understand resource for site administrators to use when reviewing user authorizations. ITS will conduct annual reviews of both the RACF Authorization and SAP Roles legends.

3. Ensure Controls Are In Place To Revoke Access For Food Service Managers Who Have Transferred To Another Location

Food Service Managers are employed by the District to manage School Cafeterias. They are allowed access to certain student information related to eligibility for free or reduced lunches. An employee from the Department of Food and Nutrition requests Food Service Managers' access to specific locations with assistance from ITS.

In our site visits and testing of 13 schools, we found three Food Service Managers that had a total of five Legacy authorizations, who had transferred to another school or location, but whose Legacy access had not been revoked.

A Food and Nutrition Director had historically performed the monthly reconciliation for Food Service Manager access to systems and applications and worked with ITS staff to revoke access when a manager transferred. However, that Food Service Director retired in September 2016, and according to senior ITS staff, that reconciliation and removal process has not been consistently performed since then.

Also, site administrators were not aware that they had the authority to revoke Food Service Manager authorizations and believed this was a function of the Department of Food and Nutrition.

Not timely removing these authorizations could increase the risk of unauthorized access to Personally Identifiable Information (PII) of students.

<u>Recommendation</u>

3.1. The Department of Food and Nutrition should ensure that staff are assigned to continue performing the Food Service Manager authorization reconciliation and removal processes. School Operations should also inform and train site administrators on how to terminate Food Service Managers' access after they leave the site administrator's location.

Responsible Departments: **School Operations,**
Department of Food and Nutrition

Management's Response:

The Department of Food and Nutrition Administrative Director will designate the responsibility of overseeing the reconciliation and removal process. Additionally, the Department of Food and Nutrition will provide resources to site administrators for terminating Food Service Managers' access after they leave the Site Administrator's location and update.

4. Site Administrators Experience Difficulty Generating Reconciliation Reports

In interviews conducted by OMCA staff, almost half (i.e., 10 of 21) of site administrators cited difficultly and/or unfamiliarity with the process of generating the Legacy RACF and/or SAP Security Roles reports.

Some site administrators stated that the Legacy RACF reports are not always available on the same date each month and are unsure of when they are available. Some also stated they were unsure of the report's exact location or how to generate the reports.

ITS states that the Legacy RACF reconciliation reports are programmed to run on the second Tuesday of the month versus a specific date each month. However, ITS stated that due to technical issues, the jobs may be running on the second Wednesday of the month. Some site administrators are also not aware that the SAP Security Roles reports are available in real time and can be generated at any time of the month. Further, site administrators may not be adequately trained on how to obtain/generate the reports.

<u>Recommendation</u>

4.1. While site administrators are ultimately responsible for monthly reconciling and removing inappropriate authorizations, ITS should consider programming that would generate Legacy RACF and SAP Security Roles reconciliation reports that are automatically and predictably sent to a site administrator's email every month. Alternatively, an email reminder could be sent every month informing site administrators that the reports are available with clear instructions on how to access each report.

Responsible Departments: ITS, School Operations

Management's Response:

ITS will facilitate the reconciliation process for the Site Administrators responsible for granting access and removing inappropriate authorizations by sending monthly email reminders to all Quad-A administrators with clear instructions on how to access each report in order to inform them of the availability of the RACF Authorization Report and to remind them of their responsibility to generate the monthly SAP Roles Report. Furthermore, School Operations has established guidelines in the School Operations Management Guide for principals to implement a calendar reminder to conduct monthly review and/or reconciliation of authorizations in both Legacy and SAP.

APPENDIX

MANAGEMENT’S RESPONSE MEMORANDUM

MEMORANDUM **August 23, 2019**

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

FROM: Ms. Valtena G. Brown, Deputy Superintendent/Chief Operating Officer
School Operations

Marie Izquierdo, Chief Academic Officer
Office of Academics and Transformation

SUBJECT: RESPONSE TO AUDIT OF LEGACY SAP SYSTEMS DISTRICT-WIDE SECURITY CONTROLS ROLES AND ACCESS MANAGEMENT

The Office of Academics and Transformation, which includes Information Technology Systems (ITS), and School Operations have reviewed the audit findings and recommendations cited in the 2018-2019 Audit of Legacy/SAP Systems – District-Wide Security Controls, Roles, and Access Management report.

Below is a joint management response of the bureaus represented in the report that outlines the corrective and preventative actions taken by School Operations and the Office of Academics and Transformation through ITS:

1.1 School Operations will provide a review to site administrators through Scaled Leadership to ensure they perform monthly reconciliations of user authorization and minimize authorization/access to Legacy/SAP applications. Moving forward, weekly briefings regarding these applications and security updates will be published each year (as applicable) as a compliance feature in the School Operations Management Guide.

1.2 ITS will redistribute weekly briefings with important security updates as appropriate. The Network Security Standards will continue to be updated and distributed as necessary. Significant changes to the NSS will prompt a weekly briefing to all employees to raise awareness to changes that may have a significant impact on regular user functions.

2.1 ITS is in the process of updating the RACF Authorization and SAP Roles legends in order to provide a comprehensive and easy-to-understand resource for site administrators to use when reviewing user authorizations. ITS will conduct annual reviews of both the RACF Authorization and SAP Roles legends.

3.1 The Department of Food and Nutrition Administrator Director will designate the responsibility of overseeing the reconciliation and removal process. Additionally, the Department of Food and Nutrition will provide resources to site administrators for terminating Food Service Managers' access after they leave the Site Administrator's location and update.

4.1 ITS will facilitate the reconciliation process for the Site Administrators responsible for granting access and removing inappropriate authorizations by sending monthly email reminders to all Quad-A administrators with clear instructions on how to access each report in order to inform them of the availability of the RACF Authorization Report and to remind them of their responsibility to generate the monthly SAP Roles Report. Furthermore, School Operations has established guidelines in the School Operations Management Guide for principals to implement a calendar reminder to conduct monthly review and/or reconciliation of authorizations in both Legacy and SAP.

If you have any questions, please contact Ms. Valtena G. Brown, Deputy Superintendent/Chief Operating Officer, School Operations, or Marie Izquierdo, Chief Academic Officer, Office of Academics and Transformation, at 305 995-1451, or Gene Baker, Chief Information Officer, Division of Information Technology Services, at 305 995-3750.

VGB/MI:cg/efg
M012

cc Jon Goodman
Eugene Baker
Region Superintendents
Cynthia Gracia
Ernesto F. Gonzalez

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, maritl 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

Miami-Dade County Public Schools

Internal Audit Report

Audit of Legacy/SAP Systems District-Wide Security Controls, Roles and Access Management

SEPTEMBER 2019

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