STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-039
October 2019

# SEMINOLE COUNTY DISTRICT SCHOOL BOARD

## Oracle PeopleSoft Applications and Skyward Student Information System


Sherrill F. Norman, CPA
Auditor General

## Board Members and Superintendent

During the period, October 2018 through February 2019, Dr. Walter Griffin served as Superintendent of the Seminole County Schools and the following individuals served as School Board Members.

| | District No. |
|---|---|
| Kristine Kraus from 11-20-2018 | 1 |
| Jeffrey Bauer to 02-07-2018 [a] | 1 |
| Karen Almond, Vice Chair from 11-20-2018 | 2 |
| Abby Sanchez | 3 |
| Amy Pennock from 11-20-2018 | 4 |
| Amy Lockhart to 11-19-2018, Chair through 11-19-2018 | 4 |
| Dr. Tina Calderone, Chair from 11-20-18, Vice Chair through 11-19-2018 | 5 |

[a] Position vacant from 02-07-2018, to 11-19-2018.

The team leader was Vikki Mathews, CISA, and the audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us by telephone at (850) 412-2926.

This report and other reports prepared by the Auditor General are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

**State of Florida Auditor General**

**Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722**

# SEMINOLE COUNTY DISTRICT SCHOOL BOARD

## Oracle PeopleSoft Applications and Skyward Student Information System

## SUMMARY

This operational audit of Seminole County District School Board (District) focused on evaluating selected information technology (IT) controls applicable to the Oracle PeopleSoft Applications (PeopleSoft Applications) used to process and report its finance and human resource (HR) transactions and the Skyward Student Information System (Skyward) for the recording, processing, and reporting of student-related transactions and the infrastructure supporting PeopleSoft Applications and Skyward. As summarized below, our audit disclosed areas in which improvements in the District controls and operational processes are needed.

**Finding 1:** District controls related to application security management need improvement to ensure that access privileges granted within Skyward are necessary and appropriate.

**Finding 2:** District security controls related to mobile device management need improvement.

**Finding 3:** District IT security controls related to user authentication, user account management, network account management, and logging and monitoring of system activity need improvement to ensure the confidentiality, integrity, and availability of District data and IT resources.

## BACKGROUND

The Seminole County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education. The governing body of the District is the Seminole County District School Board (Board), which is comprised of five elected members. The appointed Superintendent of Schools is the executive officer of the Board. During the 2018-19 fiscal year, the District had 72 centers and schools other than charter schools, 4 charter schools, and reported 80,925 unweighted full-time equivalent students.

The District uses Oracle PeopleSoft Applications (PeopleSoft Applications) to process and report its finance and human resources (HR) transactions and the Skyward Student Information System (Skyward) for the recording, processing, and reporting of student-related transactions. In addition, the District maintains and manages the network domain, application and database servers, and database management systems supporting PeopleSoft Applications and Skyward.

## FINDINGS AND RECOMMENDATIONS

### Finding 1: Application Security Management

Effective application security management provides a framework for managing risk, developing policies, and monitoring the adequacy of application-related controls. As part of application security management, a comprehensive, documented security design ensures, through the identification of sensitive transactions and separation of duties, that security roles are defined appropriately so that users are not

granted excessive or inappropriate access. In addition, periodic reviews of access privileges associated with security roles help ensure that access privileges provided to each security role remain appropriate and necessary. Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls include granting employees access to IT resources based on a demonstrated need to view, change, or delete data and restricting employees from performing incompatible functions or functions outside of their areas of responsibility.

IT access privileges within Skyward are controlled by assigning groups to employees. Groups are created by the District and include menus with defined permissions to view or edit specific screens and fields. Groups are defined at the District level and at the school level allowing employees assigned access privileges across the District or at one or more school levels. Our audit procedures disclosed that the District's management of Skyward access privileges need improvement. Specifically:

- As of July 2019, the District had not performed a comprehensive review of employee access privileges assigned within Skyward. Skyward reports of access privileges assigned by group or of employees and their assigned groups are voluminous making the reports inefficient to produce and difficult for District staff to effectively use for review. In response to our audit inquiry, District management indicated that targeted access reviews (i.e., selected groups or employees) would begin during quarterly security meetings.
- Of 518 employees having access to a selected group,[1] we selected 26 employees and found that 21 of the 26 employees had unnecessary access to some or all of the student information granted through the group. District management stated that the employees were assigned the group because the additional access supports the employees current job duties, and the District intends to explore the availability of additional restrictions for accessing attendance, discipline, health, and grade information. Subsequent to our audit inquiry, District management removed Skyward access from 3 of the 21 employees.
- Nineteen employees were assigned systemwide access privileges that allowed update access to all functions within Skyward, including transaction origination, correction, and changes to student data, security tables, configuration files, and utilities. Six of the 19 employees were assigned State reporting responsibilities and the other 13 employees were assigned IT responsibilities. In response to our audit inquiry, District management removed systemwide access from 1 of the employees with State reporting responsibilities but indicated that the other 18 employees needed the access for installing updates, running certain utilities, troubleshooting problems, and investigating State reporting errors. However, each of these 18 employees' day-to-day responsibilities did not require complete update access privileges to Skyward and such privileges are contrary to an appropriate separation of end-user and technical support functions.

Appropriately restricted access privileges help protect District data and IT resources from unauthorized modification, loss, and disclosure.

**Recommendation: We recommend that District management establish procedures requiring periodic review of access privileges granted within Skyward and ensure that the access privileges granted are necessary and appropriate for the employee's assigned responsibilities.**

[1] The group selected was assigned to employees at the District level or at one of three selected schools and allowed access to discipline, health, attendance, and grading information.

## Finding 2: Mobile Device Management

Effective mobile device management includes establishing policies and procedures related to how the entity will manage the configuration and security of each mobile device (cellular telephone, laptop, or tablet), whether entity or employee-owned, before allowing the device to access entity data and IT resources. Well-designed policies and procedures include defined security requirements for mobile devices pertaining to device encryption, current standard configuration, patching, anti-virus protection, and passcode protection. In addition, established policies and procedures should define the responsibilities of the entity and the user when mobile devices are used to connect to an entity's network and IT resources. The effective implementation of such policies and procedures requires an inventory of all mobile devices authorized to connect to an entity's network environment and the ability to systematically enforce defined security requirements.

District Board Policy 7542, *Access to Technology Resources from Personal Communication Devices*, allows employee access to confidential and sensitive data on the District's network using personally owned mobile devices. However, the District had not established security requirements, such as minimum operating system requirements, use of a passcode, device encryption, and current virus protection for mobile devices. In addition, the District did not maintain an inventory of the personally owned mobile devices authorized to connect to the District's network environment or have the ability to systematically enforce security requirements for these devices thereby limiting the prevention and detection of unauthorized mobile devices' access to the network. Further, the District had not established policies and procedures for user responsibilities regarding the handling of confidential and sensitive data on personally owned mobile devices, such as downloading or copying confidential or sensitive data to the device and reporting the loss of the device or compromise of data, or for District-required actions for responding to incidents of lost or stolen devices.

In response to our audit inquiries, District management indicated that a directive, with an implementation date of June 30, 2019, was created regarding the use of personally owned mobile devices connected to the District's network, including device requirements, user responsibilities, and conditions for use.

Effective mobile device management through established and enforceable security requirements and user responsibilities help ensure the confidentiality, integrity, and availability of District data and IT resources.

**Recommendation: We recommend that District management continue efforts to establish minimum security requirements for personally owned mobile devices connecting to the District's network and also establish policies and procedures for the use of the mobile devices, including the handling of confidential and sensitive District data on mobile devices, user responsibilities for loss or data compromise, and District actions in response to incidents of lost or stolen devices. We also recommend that District management maintain an inventory of all personally owned mobile devices authorized to connect to the District's network and systematically enforce established security requirements for those devices.**

### Finding 3: Security Controls – User Authentication, User Account Management, Network Account Management, and Logging and Monitoring

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication, user account management, network account management, and logging and monitoring need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the confidentiality of District data and related IT resources. However, we have notified appropriate District management of the specific issues.

Without appropriate security controls related to user authentication, user account management, network account management, and logging and monitoring, the risk is increased that the confidentiality, integrity, and availability of District data and related IT resources may be compromised.

**Recommendation: We recommend that District management improve IT security controls related to user authentication, user account management, network account management, and logging and monitoring to ensure the confidentiality, integrity, and availability of District data and IT resources.**

## *OBJECTIVES, SCOPE, AND METHODOLOGY*

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from October 2018 through July 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to the Oracle PeopleSoft Applications (PeopleSoft Applications) and Skyward Student Information System (Skyward) during the period October 2018 through February 2019, and selected actions subsequent thereto. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way

as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT systems and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an understanding of the IT systems and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed District staff and reviewed District records to obtain an understanding of District operations for the PeopleSoft Applications and Skyward infrastructure, including authentication, logical controls, and logging and monitoring of the network, application and database servers, and the database management systems; Skyward application logical controls, change management, and logging and monitoring; data and business process flows within Skyward; and mobile device management for personally owned mobile devices connecting to the District's network.
- Evaluated the effectiveness of logical access controls, including the periodic reviews for the network domains, Windows application and database servers, and databases supporting the PeopleSoft Applications and Skyward.
- Examined and evaluated the appropriateness of administrative privileges for the District's network forest and child domain, as of October 16, 2018; the Windows application and database servers supporting PeopleSoft Applications and Skyward, as of October 22, 2018; and the root domain, as of December 5, 2018.
- Examined and evaluated user authentication controls related to the password change interval for 331 network domain accounts, as of October 16, 2018.
- Examined and evaluated the appropriateness of accounts and privileges assigned on the finance and human resources (HR) databases supporting the PeopleSoft Applications as of October 16, 2018. Specifically, we examined and evaluated:
    - 66 accounts assigned selected administrative privileges on the finance database.
    - 68 accounts assigned selected administrative privileges on the HR database.
    - 31 accounts assigned to the finance database with default passwords.

- 31 accounts assigned to the HR database with default passwords.

- Evaluated the effectiveness of logical controls assigned within Skyward, including periodic reviews of access privileges and the use of Systemwide access.
- Examined and evaluated the appropriateness of access privileges, as of March 28, 2019, granted within Skyward for 26 employees.
- Evaluated user authentication controls related to the District IT Infrastructure supporting PeopleSoft Applications and Skyward.
- Evaluated the effectiveness of District system software and network infrastructure component change control procedures related to the District's IT infrastructure applicable to PeopleSoft Applications and Skyward.
- Evaluated the effectiveness of the District's change management controls related to the authorization, testing, and approval of PeopleSoft Applications and Skyward application changes.
- Examined and evaluated the appropriateness of 17 PeopleSoft Applications changes implemented during the period October 1, 2018, through December 11, 2018.
- Examined and evaluated the appropriateness of 10 Skyward advanced data fix changes implemented during the period October 1, 2018, through January 11, 2019.
- Evaluated the effectiveness of the District's vulnerability management (logging, monitoring, and remediation) for the network, application and database servers, and critical network infrastructure components supporting PeopleSoft Applications and Skyward.
- Evaluated the effectiveness of the District's logging and monitoring controls, including actions performed by privileged users, for the databases supporting PeopleSoft Applications and Skyward.
- Evaluated the effectiveness of the District's logging and monitoring controls related to student information within Skyward.
- Evaluated the effectiveness of the District's mobile device security plan, including security and configuration requirements and District- and user-defined responsibilities.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

## AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

# MANAGEMENT'S RESPONSE

Seminole County Public Schools

WALT GRIFFIN, Ed.D.
*Superintendent*

**Educational Support Center**
400 E. Lake Mary Boulevard
Sanford, Florida 32773-7127
Phone: (407) 320-0000
Fax: (407) 320-0281

*Visit Our Web Site*
www.scps.us

October 14, 2019

Sherrill F. Norman, CPA
Auditor General
State of Florida
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Re: Response to Information Technology Operational Audit Findings

Dear Ms. Norman:

Attached are our responses to the findings in the I.T. operational audit completed by your office. Although audits bring about additional requirements in an already thinly resourced organization, they do provide an opportunity for us to examine our I.T. practices and protocol for opportunities to improve how we manage our vast technology systems. I want to compliment your staff for their thorough work and professional demeanor.

Sincerely,

Walt Griffin, Ed. D.

## DISTRICT RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS

**District**: Seminole County **Audit Report No.:** TBD **Report Date:** September 30, 2019

| **Finding # 1**<br>**Application Security Management** | **Recommendation:**<br>**That District management establish procedures requiring periodic review of access privileges granted within Skyward and ensure that the access privileges granted are necessary and appropriate for the employee's assigned responsibilities** |
|---|---|
| **Response:**<br>The School Board of Seminole County (SBSC) concurs with this recommendation and is implementing a quarterly review of user access in its Skyward student information system (SIS). The Administrator, Information Security Officer (AISO) is in charge of scheduling and conducting quarterly security reviews. Key stakeholders who will review Skyward user access include district level executive leadership, the Chief Technology Officer (CTO), and the Application Support Manger who is responsible for oversight of the SIS. If, in the course of these quarterly reviews, an individual is determined to have unnecessary access to data, then the account will be modified within two (2) hours following the review. | |

| **Finding # 2**<br>**Mobile Device Management** | **Recommendation:**<br>**That District management continue efforts to establish minimum security requirements for personally owned mobile devices connecting to the District's network and also establish policies and procedures for the use of the mobile devices, including the handling of confidential and sensitive District data on mobile devices, user responsibilities for loss or data compromise, and District actions in response to incidents of lost or stolen devices. We also recommend that District management maintain an inventory of all personally owned mobile devices authorized to connect to the District's network and systematically enforce established security requirements for those devices.** |
|---|---|
| **Response:**<br>The School Board of Seminole County (SBSC) agrees with this recommendation. District management created a directive in June 2019 regarding the use of personally owned mobile devices connected to the District's network, including device requirements, user responsibilities, and conditions for use. The District continues to investigate Network Access Control (NAC) solutions with the goal being to acquire and implement a solution by the start of the 2020-21 school year. This will allow the District to maintain an inventory of all personally owned mobile devices that connect to its network and systematically enforce established security requirements for these devices. SBSC acquired Microsoft Office for Education A5 licensing for all full-time employees in July 2019. This licensing includes the Azure Information Protection (AIP) component for document classification and labelling (e.g. Confidential vs. Published). The District intends to complete district training and a staged rollout of AIP to all users by the end of the 2019-20 school year. AIP will operate in conjunction with Microsoft Cloud Application Security (CAS) and Data Loss Prevention (DLP) to further insure sensitive information cannot be improperly accessed by staff via personally owned mobile devices. | |

| **Finding # 3**<br>**Security Controls – User Authentication, User Account Management, Network Account Management, and Logging and Monitoring** | **Recommendation:**<br>**That District management improve IT security controls related to user authentication, user account management, network account management, and logging and monitoring to ensure the confidentiality, integrity, and availability of District data and IT resources.** |
|---|---|
| **Response:**<br>The School Board of Seminole County (SBSC) concurs with this recommendation. SBSC acquired Microsoft Office for Education A5 licensing for all full-time employees in July 2019. This licensing includes a Multi-Factor Authentication (MFA) capability for Azure connected services like Office 365. The District intends to complete district training and a staged rollout of MFA to all employees by the end of the 2019-20 school year. The District will also implement additional security measures in support of user authentication for its ERP and SIS applications. | |