

STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2025-123
February 2025

**VOLUSIA COUNTY
DISTRICT SCHOOL BOARD**



Sherrill F. Norman, CPA
Auditor General

Board Members and Superintendent

During the 2023-24 fiscal year, Dr. Carmen J. Balgobin served as Superintendent of the Volusia County Schools and the following individuals served as School Board Members:

	<u>District No.</u>
Jamie M. Haynes, Chair	1
Anita Burnette, Vice Chair	2
Jessie Thompson	3
Carl Persis	4
Ruben Colón	5

The team leader was Nicole E. Ryals, CPA, and the audit was supervised by Keith A. Wolfe, CPA.

Please address inquiries regarding this report to Edward A. Waller, CPA, Audit Manager, by e-mail at tedwaller@aud.state.fl.us or by telephone at (850) 412-2887.

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

VOLUSIA COUNTY DISTRICT SCHOOL BOARD

SUMMARY

This operational audit of the Volusia County School District (District) focused on selected District processes and administrative activities and included a follow-up on findings noted in our report No. 2023-002. Our operational audit disclosed the following:

Finding 1: District controls did not always ensure legally sufficient complaints against District teachers and administrators were timely filed with the Florida Department of Education.

Finding 2: District controls over purchasing cards need improvement.

Finding 3: As similarly noted in our report No. 2023-002, some unnecessary information technology (IT) user access privileges existed that increased the risk for unauthorized disclosure of sensitive student personal information to occur.

Finding 4: District security management controls continue to need improvement.

Finding 5: As of July 2024, the District disaster recovery plan had not updated or tested since the 2015 calendar year.

Finding 6: The District needs to establish a comprehensive IT risk assessment to provide a documented basis for managing IT risks.

BACKGROUND

The Volusia County School District (District) is part of the State system of public education under the general direction of the Florida Department of Education and is governed by State law and State Board of Education rules. Geographic boundaries of the District correspond with those of Volusia County. The governing body of the District is the Volusia County District School Board (Board), which is composed of five elected members. The appointed Superintendent of Schools is the Executive Officer of the Board. During the 2023-24 fiscal year, the District operated 68 elementary, middle, high, and specialized schools; sponsored 6 charter schools; and reported 65,360 unweighted full-time equivalent students.

FINDINGS AND RECOMMENDATIONS

Finding 1: Employee Misconduct

State law¹ requires the District to file in writing with the Florida Department of Education (FDOE) all legally sufficient complaints against District teachers and administrators within 30 days after the date on which subject matter of the complaint comes to the attention of the District. According to District personnel, school administrators or the District Office may receive complaints by telephone, e-mail, or in person. The complaints are forwarded to District Professional Standards Department personnel to investigate the

¹ Section 1012.796(1)(d), Florida Statutes.

severity, potential ramification, and legal sufficiency of the complaint and, if deemed legally sufficient, the complaints are filed with the FDOE.

During the 2023-24 fiscal year, the District filed with the FDOE 31 legally sufficient complaints against teachers and administrators affecting the health, safety, and welfare of students. As part of our audit, we examined District records supporting the complaints filed with the FDOE and found that 16 legally sufficient complaints were filed 37 to 173 days, or an average of 64 days, after the complaints came to the attention of the District.

In response to our inquiries, District personnel indicated that allegations of misconduct are not deemed legally sufficient until the allegations are properly investigated and that the 30-day period for reporting to the FDOE begins after the legal sufficiency determination is made. Notwithstanding, while the determination of legal sufficiency is contemplated to occur within the 30-day filing allowance and no provision appears to address complaints that develop legal sufficiency outside the statutory window, the legal requirement to report the complaints becomes effective on the date that the complaint comes to the attention of the District.

Absent effective controls to ensure that complaints are timely filed, the District cannot demonstrate compliance with State law, the FDOE's ability to monitor the complaints is limited, and the District cannot demonstrate that all appropriate measures have been taken to promote student and staff safety.

Recommendation: The District should enhance procedures to ensure compliance with State law by filing with the FDOE all legally sufficient complaints against teachers and administrators within 30 days after the subject matter of the complaint comes to the attention of the District.

Finding 2: Purchasing Cards

The District *Purchasing Card Manual (Manual)* provides that the intent of purchasing cards (P-cards) is to allow schools and departments the flexibility to purchase goods and services directly from vendors without issuing a District purchase order. The *Manual* requires employees who are assigned P-cards to sign P-card agreements to evidence that the employee, for example, accepts responsibility for the card and agrees to use the card in accordance with the *Manual*. For P-cards assigned to school or department sites, principals or department heads must sign the agreements and the designated site reconciler is responsible for controlling use of site P-cards and recording who requests, uses, and returns the card.

P-card users must provide support for P-card expenditures to the respective site reconciler, and the site reconciler is responsible for reviewing, approving, or rejecting P-card expenditures through the bank online platform and uploading documentation supporting the approved expenditures. Finance Department personnel are to review coding for P-card expenditures and ensure documentation is attached in the bank online platform. The principal or department head is responsible for documenting secondary review and approval of the monthly P-card expenditures by signing monthly P-card bank statements and resolving any questionable expenditures with applicable P-card users.

The *Manual* specifies that, upon a cardholder's separation from employment, the site reconciler is to complete and submit to the Purchasing Department a *P-card Cancellation Form* to initiate the cancellation process with the bank. The principal, department head, or Human Resources Department is to collect the employee's P-card and deliver the card to the Purchasing Department for destruction.

During the 2023-24 fiscal year, the District incurred P-card expenditures totaling \$6.3 million and had 363 P-cards, including 357 site P-cards assigned to 123 site reconcilers for school or department use. We evaluated District P-card processes and found that controls over P-cards could be improved. Specifically:

- Neither site reconcilers nor the employees who use site P-cards sign P-card agreements or other records documenting accepted responsibility for the P-card and its proper use. In response to our inquiry, District personnel indicated that site P-card users were not required to document acceptance of responsibility for P-card use.
- We requested for examination District records supporting 17 selected site P-card expenditures totaling \$35,132 to identify who requested and used the site P-cards. However, for 16 of those expenditures totaling \$18,106, District records identifying the P-card user were not provided. According to District personnel, records supporting site P-card use were sometimes missing or not completed due to employee turnover and because decentralized locations did not always maintain those records.
- To evaluate the propriety of P-card charges, we requested for examination District records supporting 41 site P-card expenditures totaling \$52,927. We found that, for 20 of the P-card expenditures, ranging from \$12 to \$11,861 and totaling \$17,589 (33 percent of the expenditures evaluated), District records did not demonstrate secondary review and approval of the purchases. We also found that District records did not identify the public purpose for 18 of the P-card expenditures totaling \$4,595 (9 percent of the expenditures evaluated),² including charges for food (\$1,641), a television (\$1,327), bicycle maintenance (\$830), decorations (\$507), and various small dollar items. According to District personnel, secondary review and approval was not always documented because of employee turnover. District personnel also indicated that P-card expenditures were for educational purposes although the purposes were not always documented.
- To determine whether P-cards were promptly canceled after a cardholder's employment separation or when a P-card was no longer needed, we examined District records supporting the 36 P-card cancellations during the 2023-24 fiscal year. We found that the District did not employ cancellation procedures when 17 cardholders separated from District employment and the bank administering the P-card program subsequently canceled those cards when they expired. The cancellations ranged from 3 to 25 months, or an average of 19 months, after the cardholders' respective employment separation dates. For another 11 former employees, the District canceled P-cards 2 to 34 months, or an average of 10 months after the cardholders' respective employment separation dates. The delays occurred primarily because site reconcilers did not consistently comply with the *Manual* by promptly completing and submitting P-card cancellation forms but relied on the bank to cancel expired P-cards.

Moreover, 54 P-cards had no activity during the 2023-24 fiscal year and District records did not demonstrate any evaluation or basis for maintaining the P-cards. While our audit procedures disclosed that P-cards were not used after individuals separated from District employment, our procedures cannot replace District responsibility and procedures for properly controlling P-card cancellations and inactivity.

Without effective controls over P-cards, P-card users may not understand or have incentive to comply with the *Manual* requirements and there is an increased risk of P-card waste, fraud, and abuse. Subsequent to our inquiries, in October 2024 District personnel began reducing the number of site P-cards and increasing the number of employee P-cards.

² Four expenditures totaling \$846 without a documented public purpose were included in the 20 expenditures without documented secondary review and approval.

Recommendation: The District should ensure effective controls are employed for P-cards. Specifically, such controls should include:

- Documented receipt and acknowledgment of responsibility for site P-cards by those who use them.
- Documented secondary review and approval of site P-card purchases and maintenance of records supporting the public purpose for all P-card purchases.
- The prompt cancellation of P-cards:
 - For cardholders who separate from District employment.
 - When P-cards are inactive for an extended period or maintenance of records evidencing the continued need for those P-cards.

Finding 3: Information Technology User Access Privileges to Sensitive Student Information

The Legislature has recognized in State law³ that social security numbers (SSNs) can be used to acquire sensitive personal information, the release of which could result in fraud against individuals or cause other financial or personal harm. Therefore, public entities are required to provide extra care in maintaining the confidential status of such information. Effective controls restrict individuals from accessing information unnecessary for their assigned job duties and provide for documented, periodic evaluations of information technology (IT) user access privileges to help prevent individuals from accessing sensitive personal information inconsistent with their responsibilities.

Student SSNs are included in the student records maintained within the District student information system (SIS) to, for example, register newly enrolled students and transmit that information to the Florida Department of Education through a secure-file procedure and provide student transcripts to colleges, universities, and potential employers based on authorized requests. Board policies⁴ authorize designated District school officials access to student records in the exercise of a legitimate educational interest.

Our examination of District records disclosed that, as of July 2024, the District SIS contained sensitive personal information for 185,124 former and 47,025 current students and 573 District users had access to the former and current student information. As part of our audit, we inquired of District personnel and examined District records supporting the IT user access privileges for all 573 users with access privileges to the sensitive information of students. We found that District records did not demonstrate the need for 517 users, such as individuals who worked for the SIS provider, teachers, and office specialists, to have access privileges to the sensitive information of former or current students. In response to our inquiries, District personnel indicated that, although periodic evaluations of access privileges had been performed, high staff turnover contributed to only evaluating access to one field in the SIS and not the other fields where student SSNs are stored.

The existence of unnecessary IT user access privileges increases the risk of unauthorized disclosure of sensitive personal information and the possibility that such information may be used to commit fraud against former or current District students. Subsequent to our inquiry, in July 2024 District personnel

³ Section 119.07(5)(a), Florida Statutes.

⁴ Board Policy 201, *Student Records*.

removed the inappropriate access privileges for all 517 users. Similar findings were noted in our report Nos. 2023-002 and 2019-011.

Recommendation: District management should continue efforts to ensure that sensitive personal information maintained by the District is properly safeguarded. Such efforts should include documenting periodic evaluations of IT user access privileges for all areas of the SIS containing student SSNs and timely removing any inappropriate or unnecessary access privileges detected.

Finding 4: Information Technology Security Management

Effective security management includes policies and procedures that ensure risk reduction and compliance with applicable standards, guidance, and District-determined system configuration requirements and outline the duties of those responsible for overseeing security and those who own, use, or rely on District IT resources.

In January 2022, the former District Chief Information Officer (CIO) began drafting an *Information and Technology Services Directives, Standards, Guidelines, and Procedures Manual* to address network, server, and endpoint security, access, and other cybersecurity controls. The intent of the *Manual* was to underscore the CIO's responsibility for operating a security program to effectively manage risk and ensure the protection of District IT systems through a set of directives documenting expectations for achieving the underlying Board-approved policies over IT areas. Implementation of certain directives relied on detailing requirements or procedures within a standard. However, the former CIO resigned in April 2022, the current Chief Technology Officer (CTO) began employment in July 2022, and as of September 2024, standards had not been developed for directives, including encryption, configuration management, electronic data disposal, endpoint, network, and server security, information classification and protection, and logging.

In addition, during the 2023-24 fiscal year, a cyber security incident response plan, following the best practice recommendations from the National Institute of Standards and Technology, had not been developed and approved to mitigate cybersecurity incidents affecting District IT resources. Subsequently, in July 2024, such a plan was developed; however, as of December 2024, the plan had not been approved by the Board.

In response to our inquiries, District personnel indicated that security management procedures had not been developed due to high staff turnover in IT positions, including the CIO and CTO positions. Notwithstanding, without effective security management, including defined requirements and procedures for implementing security directives, the risk is increased that controls designed to ensure the confidentiality, integrity, and availability of District data and IT resources will not be followed consistently or in accordance with management's expectations, especially during periods of high staff turnover. A similar finding was noted in report No. 2023-002.

Recommendation: District management should continue to develop policies and procedures for IT security management to include all corresponding standards.

Finding 5: Information Technology Disaster Recovery

An important element of an effective internal control system over IT operations is a disaster recovery plan to help minimize data and asset loss in the event of a major hardware or software failure. A disaster recovery plan should identify key recovery personnel; critical data, processes, and applications; steps to reestablish connectivity with the host vendor; and step-by-step procedures for recovery. In addition, plan elements should be tested periodically to disclose any areas not addressed and to facilitate proper conduct in an actual disruption of IT operations.

The District receives financial IT services through a Web-based application that is vendor hosted, while the District hosts the payroll application and maintains backups of critical files. In response to our inquiry, District personnel indicated that, as of July 2024, the District disaster recovery plan had not been updated or tested since 2015 due to staff turnover within the IT Department. In addition, District personnel indicated that the District was beginning to transition to a new enterprise resource planning system for both the finance and payroll applications and plans to update the disaster recovery plan during the 2025-26 fiscal year. Notwithstanding, as of July 2024, the District had not updated or tested the disaster recovery plan to ensure that it included key elements such as key recovery personnel; critical data, processes, and applications; steps to reestablish connectivity with the host vendor; and step-by-step procedures for recovery.

Without an up-to-date and tested disaster recovery plan that identifies critical elements for recovery, District efforts to minimize the impact of, and timely recover from, a disaster or a disruption of IT operations may be hindered.

Recommendation: To provide for continuing critical operations in the event of a major hardware or software failure, District personnel should update the District comprehensive disaster recovery plan to ensure that it includes the identity of key recovery personnel; critical data, processes, and applications; steps to reestablish connectivity with the host vendor; and step-by-step procedures for recovery. In addition, the District should test the plan at least annually.

Finding 6: Information Technology Risk Assessment

Management of IT risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps entity personnel identify and understand the greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. A comprehensive IT risk assessment should consider specific threats and vulnerabilities, and the severity of such threats and vulnerabilities, at the Districtwide, system, and application levels and document the range of risks that District systems and data may be subject to, including those posed by internal and external users. IT risk assessments help support management's decisions in establishing cost-effective measures to mitigate risk and, where appropriate, formally accept residual risk.

In response to our inquiries, District personnel indicated that they had considered external and internal risks; however, due to employee turnover, documentation was not maintained to evidence conduct of a comprehensive IT risk assessment. The absence of a comprehensive IT risk assessment may lessen the District's assurance that all likely threats and vulnerabilities have been identified, the most significant

risks have been addressed, and appropriate decisions have been made regarding which risks to accept and which risks to mitigate through appropriate controls.

Recommendation: The District should conduct a comprehensive IT risk assessment to provide a documented basis for managing IT-related risks.

PRIOR AUDIT FOLLOW-UP

The District had taken corrective actions for findings included in our report No. 2023-002 except as noted in Findings 3 and 4 and shown in Table 1.

Table 1
Findings Also Noted in Previous Audit Reports

Finding	2020-21 Fiscal Year	2017-18 Fiscal Year
	Operational Audit Report No. 2023-002, Finding	Operational Audit Report No. 2019-211, Finding
3	5	4
4	7	Not Applicable

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 operational audit from June 2024 through November 2024 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 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.

This operational audit focused on selected District processes and administrative activities. For those areas, our audit objectives were to:

- Evaluate management’s performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management’s control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2023-002.
- 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 those areas included within the scope of the audit, weaknesses in management's internal controls significant to our audit objectives; instances of noncompliance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines; 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 transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our 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 our audit; obtaining an understanding of the program, activity, or function; identifying and evaluating internal controls significant to our audit objectives; 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 our audit findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of transactions and records, as well as events and conditions, occurring during the 2023-24 fiscal year audit period, and selected District actions taken prior and subsequent thereto. Unless otherwise indicated in this report, these records and transactions 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 management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit, we:

- Reviewed applicable laws, rules, Board policies, District procedures, and other guidelines, and interviewed District personnel to obtain an understanding of applicable processes and administrative activities and the related requirements.
- Reviewed Board information technology (IT) policies and District procedures to determine whether the policies and procedures addressed certain important IT control functions, such as risk assessment, security, configuration management, logging and monitoring, system backups, and disaster recovery.
- Evaluated District procedures for maintaining and reviewing employee access to IT data and resources. We examined selected user access privileges to District enterprise resource planning (ERP) system finance and human resources (HR) applications to determine the appropriateness and necessity of the access privileges based on employee job duties and user account functions and whether the access privileges prevented the performance of incompatible duties. Specifically, we tested the access privileges for the:
 - 24 users who had update access privileges to selected critical ERP system finance application functions.

- 29 users who had update access privileges to selected critical ERP system HR application functions.

We also examined the administrator account access privileges granted and procedures for oversight of administrative accounts for the applications to determine whether these accounts had been appropriately assigned and managed.

- Evaluated District procedures to prohibit former employee access to electronic data files. Specifically, we examined District records supporting selected user access privileges for 20 of the 54 employees who had ERP system finance and HR application access and separated from District employment during the audit period to determine whether access privileges were promptly deactivated.
- Determined whether the District had a comprehensive IT disaster recovery plan in place that was designed properly, operating effectively, and had been recently tested.
- Examined selected application security settings to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Determined whether the District had established a comprehensive IT risk assessment to document the District's risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
- Determined whether an adequate, comprehensive IT security awareness and training program was in place.
- Evaluated District procedures for protecting the sensitive personal information of students, including social security numbers. Specifically, we examined the access privileges of all 573 employees who had access to sensitive personal student information to evaluate the appropriateness and necessity of the access privileges based on each employee's assigned job duties.
- Inquired whether the District had expenditures or entered into any contracts under the authority granted by a state of emergency declared or renewed during the audit period.
- From the population of expenditures totaling \$113.8 million and transfers totaling \$26.3 million for the period July 2023 through May 2024, from nonvoted capital outlay tax levy proceeds, discretionary sales tax proceeds, and other restricted capital project funds, examined documentation supporting selected expenditures and transfers totaling \$2 million and \$13.2 million, respectively, to determine District compliance with the restrictions imposed on the use of these resources, such as compliance with Section 1011.71(2), Florida Statutes.
- Examined the District Web site to determine whether the proposed, tentative, and official budgets for the audit period were prominently posted pursuant to Section 1011.035(2), Florida Statutes. In addition, we determined whether the District Web site contained, for each public school within the District and for the District, the required graphical representations of summary financial efficiency data and fiscal trend information for the previous 3 years, and a link to the Web-based fiscal transparency tool developed by the Florida Department of Education (FDOE).
- Examined Board minutes identifying surplus property deletions and disposals during the audit period, interviewed District personnel, and reviewed District records to evaluate the District's surplus property control procedures.
- Examined documentation supporting the District's annual tangible personal property physical inventory process for the audit period to determine whether the inventory results were reconciled to the property records, appropriate follow-up was made for any missing items, and law enforcement was timely notified for any items unlocated and considered stolen.
- Evaluated District procedures for identifying and inventorying attractive items pursuant to Florida Department of Financial Services Rules, Chapter 69I-73, Florida Administrative Code.

- Evaluated the one employee contract with severance pay provisions to determine whether the provisions complied with Section 215.425(4), Florida Statutes.
- From the compensation payments totaling \$345.1 million to 10,818 employees during the period July 2023 through May 2024, examined District records supporting compensation payments totaling \$45,609 to 30 selected employees to determine whether the rate of pay complied with the Board-approved salary schedule and whether supervisory personnel reviewed and approved employee reports of time worked.
- Examined District records for the audit period for 30 employees selected from the population of 8,076 employees to assess whether individuals who had direct contact with students were subjected to the required fingerprinting and background screening.
- Evaluated the effectiveness of Board policies and District procedures for investigating all reports of alleged misconduct by personnel if the misconduct affects the health, safety, or welfare of a student and also notifying the result of the investigation to the FDOE pursuant to Section 1001.42(7)(b)3., Florida Statutes.
- Evaluated the effectiveness of Board policies and District procedures for reporting to the FDOE personnel subject to the disqualification list in accordance with SBE Rule 6A-10.084, Florida Administrative Code.
- Examined documentation supporting the \$194,829 payment during the audit period for a new software application to determine whether the District evaluated the effectiveness and suitability of the software application prior to purchase and the purchase was made through a competitive vendor selection process.
- From the three significant construction projects with expenditures totaling \$48.2 million for the period July 2023 through May 2024, selected two construction management projects with guaranteed maximum price contracts totaling \$69.2 million and examined documentation for selected project expenditures totaling \$4.6 million to determine compliance with Board policies, District procedures, and applicable provisions of State law and rules. Specifically, we examined District records to determine whether:
 - The construction manager was properly selected pursuant to Section 255.103, Florida Statutes.
 - District personnel properly monitored subcontractor selections and licenses.
 - The architects were properly selected pursuant to Section 287.055, Florida Statutes, and adequately insured.
 - Appropriate Board policies and District procedures addressing the negotiation and monitoring of general conditions costs had been established.
 - Documentation supporting the selected payments was sufficient and complied with the contract provisions.
 - The projects progressed as planned consistent with established benchmarks and were cost effective, and the contractors performed as expected.
 - The District made use of its sales tax exemption to make direct purchases of materials or documented justification for not doing so.
- Examined District records to determine whether the Board had adopted appropriate school safety policies and the District implemented procedures to ensure the health, safety, and welfare of students and compliance with Sections 1006.07, 1006.12, and 1011.62(12), Florida Statutes.
- Examined District records to determine whether the Board had adopted appropriate mental health awareness policies and the District had implemented procedures to promote the health, safety,

and welfare of students and ensure compliance with Sections 1011.62(13) and 1012.584, Florida Statutes, and SBE Rule 6A-1.094124, Florida Administrative Code.

- From the population of purchasing card (P-card) transactions totaling \$6.3 million during the audit period, examined documentation supporting 41 selected transactions totaling \$52,927 to determine whether P-cards were administered in accordance with Board policies and District procedures. We also determined whether the District timely canceled the P-cards for the P-cards cancelled during the audit period.
- For the charter school that was terminated in the audit period, evaluated District procedures to determine whether applicable funds and property appropriately reverted to the District and whether the District did not assume debts of the school or center, except as previously agreed upon by the District.
- Examined District records for the audit period to determine whether District procedures were effective for timely distributing the correct amount of local capital improvement funds to eligible charter schools pursuant to Section 1013.62(3), Florida Statutes.
- Examined District records for the audit period to determine whether District procedures ensured that vendor information changes were properly authorized, documented, and verified.
- Determined whether non-compensation expenditures were reasonable, correctly recorded, adequately documented, for a valid District purpose, properly authorized and approved, and in compliance with applicable State laws, SBE rules, contract terms and Board policies; and applicable vendors were properly selected. Specifically, from the population of non-compensation expenditures totaling \$341.2 million for the period July 2023 through May 2024, we examined documentation supporting 30 selected payments for general expenditures totaling \$378,606.
- 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, requires that the Auditor General conduct an operational audit of each school district on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



Dr. Carmen J. Balgobin
Superintendent of Schools

School Board of Volusia County

Ms. Jamie Haynes, Chair
Mr. Ruben Colón, Vice Chair
Mrs. Donna Brosemer
Mrs. Krista Goodrich
Mrs. Jessie Thompson

To: Sherrill F. Norman, CPA, Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, Florida 32399-1450
flaudgen_audrpt_dsb@aud.state.fl.us

CC: Nicole E. Ryals, CPA
Educational Entities and Local Government Audits
State of Florida Auditor General – DeLand Office
nicoleryals@aud.state.fl.us

From: Dr. Carmen J. Balgobin, Superintendent of Schools
Volusia County School Board
cbalgobi@volusia.k12.fl.us

Date: February 20, 2025

Subject: Response to Audit Findings

The following are the responses of the Volusia County School Board (“the District”) to the six preliminary and tentative findings of the State of Florida Auditor General found in the enclosure at the end of this document. The District appreciates the findings and is working diligently to correct them. As you will see in these responses, many have already been corrected or will be soon.

Response to Audit Finding #1: Employee Misconduct

VCS acknowledges the importance of adhering to state laws and ensuring the timely filing of complaints to promote the safety and welfare of our students and staff. We understand that Section 1012.796(1)(d), Florida Statutes, mandates the District to file all legally sufficient complaints against teachers and administrators with the Florida Department of Education within 30 days of the complaint coming to the District's attention. We recognize that during the 2023-24 fiscal year, 16 out of 31 legally sufficient complaints were filed beyond this 30-day window, with delays ranging from 37 to 173 days.

Corrective Actions Implemented and Planned:

1. Clarification of Reporting Timeline

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

- We acknowledge the statutory requirement that the 30-day period begins when the complaint comes to the District's attention, not after the determination of legal sufficiency. We will ensure that all relevant personnel are fully aware of this requirement.
2. **Enhanced Procedures**
 - We will enhance our procedures to ensure that all complaints are promptly forwarded to the District Professional Standards Department for immediate action. This includes setting up a tracking system to monitor the timeline from the receipt of the complaint to its filing with the Florida Department of Education.
 - While determining legal sufficiency, 10- and 15-day checkpoints will be implemented for monitoring. On Day 15, the Office of Professional Standards will submit a summary report to the Florida Department of Education to ensure compliance.
 3. **Regular Reviews**
 - We will implement regular internal reviews of the timeliness of complaint filings. These will help identify any delays and ensure continuous compliance with state laws. Reviews will occur bimonthly.
 4. **Collaboration with Florida Department of Education**
 - We will work closely with the Florida Department of Education to ensure that our procedures align with their expectations and to seek guidance on any ambiguities in the reporting process.

We are committed to addressing the issues identified in your audit and to taking all necessary measures to ensure compliance with state laws. Our goal is to maintain a safe and supportive environment for our students and staff.

Response to Audit Finding #2: Purchasing Cards

The Volusia County School District (the District) acknowledges the findings related to purchasing card (P-card) controls and remains committed to strengthening oversight, accountability, and compliance with established policies and procedures.

Recognizing the importance of financial stewardship, the District proactively commissioned an **Internal Audit of the P-Card Program** for District funds, conducted by RSM US LLP, which was completed in June 2024. This audit provided a comprehensive review of P-card processes and identified key areas for improvement, many of which align with the findings noted in this operational audit. The internal audit served as a foundation for implementing necessary corrective actions to mitigate risks, improve documentation, and enhance financial controls.

Corrective Actions Implemented and Planned:

1. **Documented Receipt and Responsibility for Site P-Cards**
 - Effective immediately, all employees utilizing a site P-card must sign an acknowledgment form outlining their responsibilities.

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

- Site reconcilers will maintain a **formal check-in/check-out log** documenting who requests, uses, and returns the P-card.
 - Mandatory P-card training is being expanded to include all site users, not just reconcilers. For users of a site base card a procedure will be used to instruct the employee on the proper use of the card through checking it back in.
2. **Strengthening Documentation and Review of Purchases**
- A **secondary review and approval process** is now required for all P-card expenditures, with principals/department heads signing off on purchases before Finance finalizes payment.
 - The Finance Department conducts monthly reviews at the time the transactions are processed for payment to ensure purchases have proper supporting documentation and align with public purpose requirements.
 - The District is enhancing training for all reconcilers and purchasing approvers to reinforce compliance with **public purpose expenditure documentation**.
3. **Timely Cancellation of P-Cards for Separated Employees**
- The District has enhanced procedures to ensure that P-cards assigned to separated employees are canceled **within 10 business days** of their departure.
 - A **cross-check system** between Human Resources, Procurement, and Finance has been established to verify that departing employees do not retain active P-cards.
 - All inactive P-cards are reviewed **quarterly**, and those without valid justification for retention are deactivated.
4. **Reduction of Unused P-Cards**
- A **review of active P-cards** resulted in a reduction of the number of site-assigned P-cards in favor of individual employee-assigned P-cards, enhancing accountability.
 - Site reconcilers must now conduct **quarterly evaluations** of P-card usage and provide justification for maintaining any underutilized cards.

These corrective measures align with both the **Operational Audit** recommendations and the findings from the **FY24 Internal Audit of P-Cards**, ensuring a robust internal control structure moving forward. The District remains committed to financial transparency and compliance with best practices.

Response to Audit Finding #3: Information Technology User Access Privileges to Sensitive Student Information

VCS takes the security and privacy of our students' sensitive information very seriously and are committed to addressing the deficiencies identified in your audit. We acknowledge that effective controls are essential to restrict access to sensitive information and to ensure that only individuals with legitimate educational interests have access to such data. We understand the risks associated with unnecessary user access

P.O. BOX 2118 · 200 NORTH CLARA AVE
 DELAND, FL 32720
 (386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

privileges and the potential for unauthorized disclosure of sensitive personal information.

Corrective Actions Implemented and Planned:

1. Removal of Inappropriate Access Privileges

- As of July 2024, after review and discussions with the auditors, the District removed any unwarranted access privileges. In addition, it was clarified that most users in question could only access a partial SSN.
- Employees with the following profiles currently view a partial SSN: *Assessment District Office, Registrars, Athletics, School Counselor, Home Education Admin, In-School Suspension Facilitator, SSS Wellness Admin, FTE Specialist, SIS Support, and System Administrators.*
- SSNs can possibly be viewed in a legacy FLDOE 'Student Alias' field. There were 18 employees that had access to this field. It is only used for FLDOE verification and matching purposes. Access is now reduced to just 2 employees and is restricted to the following profile: *FTE Specialist.*

2. Periodic Evaluations

- We have implemented a more rigorous process for periodic evaluations of user access privileges. This process now includes a comprehensive review of all fields within the SIS where student SSNs are stored, ensuring that access is limited to only those with a legitimate need.

3. Documentation and Monitoring

- We are improving our documentation procedures to ensure that all evaluations of user access privileges are thoroughly recorded. Additionally, we are implementing enhanced monitoring systems to detect and address any inappropriate access promptly.

Additionally, we would like to provide further clarification on certain roles within our district that require access to student SSNs. The only employees that can view a full SSN are those with the profile 'View Full SSN' and must acquire this profile by requesting permission from their School or District leadership to ask the Security Contact to submit a Support Ticket to Account Management providing justification as to why their job role requires this access. This must also be approved by the Assistant Director, Student Information Systems. There are currently 35 employees with the following titles that have this access:

- **System Administrators:** These employees manage the software and systems processes that store and maintain all Student Information Systems (SIS) data. Their responsibilities include managing online screens, reports, update jobs, data extractions, workflows, and the configuration and management of processes for integrations with other approved applications. They need access to all data for the purposes of data verification, data movement, and troubleshooting.
- **FTE Specialists:** These employees manage the reporting of SIS data to and from the Florida Department of Education, which requires the transmission of SSNs when available.

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

- **SIS Support:** These employees directly support the Registrars and Data Entry personnel who enter and maintain the data. They provide training, procedure guides, data verification, and troubleshooting.
- **Assessment District Office:** These employees work directly with assessment organizations and vendors, some of which still use SSNs as a key element for identifying unique assessment score records. They also support district and school personnel who work with this data.

We are committed to maintaining the highest standards of data security and will continue to work diligently to safeguard the sensitive personal information of our students.

Response to Auditor Finding 4: Information Technology Security Management

We acknowledge the importance of effective security management to ensure risk reduction and compliance with applicable standards, guidance, and VCS-determined system configuration requirements. The District has modernized numerous policies and processes over the last few years including our Technology Use Policy for Students and Staff, the Student and Staff Use of AI Policy, Software Selection and Retirement Policy, and the Continuity of Operations and Recovery Plan.

Corrective Actions Implemented and Planned:

1. Staff Turnover

- The high turnover in ITS positions, including the CTO role, has impacted the continuity and completion of some policies, procedures, and standards. The transition period between the former CTO's resignation in April 2022 and the current CTO's commencement in July 2022 contributed to delays.

2. Development of Standards

- We acknowledge that as of September 2024, documented standards for encryption, configuration change management, electronic data disposal, network/server security, and logging had not been fully developed. This is an area we are actively addressing. We are committed to writing the needed standard operating procedures. A dedicated team has been assigned to this task to ensure timely completion.

3. Policy Development

- VCS will prioritize the development of standards for data encryption, configuration change management, electronic data disposal, endpoint security, network and server security, and log management during the 2025-2026 school year.

We appreciate the auditor's recommendations and are committed to enhancing our cyber security management. By developing comprehensive policies and procedures, we aim to ensure the confidentiality, integrity, and availability of District data and technical resources. We will continue to work diligently to meet these objectives and comply with all applicable standards and guidelines.

Response to Audit Finding 5: Information Technology Disaster Recovery

P.O. BOX 2118 · 200 NORTH CLARA AVE
 DELAND, FL 32720
 (386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

The District acknowledges the importance of maintaining an up-to-date and tested disaster recovery plan to ensure the continuity of critical operations in the event of a major hardware or software failure.

Corrective Actions Implemented and Planned:

1. Completion of Continuity of Operations and Recovery Plan:

- We have recently completed a new Continuity of Operations and Recovery Plan, which serves as a comprehensive disaster recovery plan for technical systems.
- The plan includes the identification of key recovery personnel, a high-level playbook to guide the recovery process, and detailed playbooks for critical services and systems. These playbooks outline the timelines, critical decisions, and procedures for reestablishing vendor connectivity and/or the recovery steps necessary to restore operations.

2. Transition to New ERP System:

- As part of our transition to a new enterprise resource planning (ERP) system for finance, HR, and payroll applications, we are integrating disaster recovery planning into the implementation process. This will ensure that the new system is supported by a robust and current disaster recovery plan.

3. Updating and Annual Testing:

- The plan will be updated when significant technological advancements or system replacements occur.
- We commit to testing the disaster recovery plan at least annually. This summer, we plan to conduct a tabletop exercise with the school district's Superintendent's Cabinet to test the plan and ensure its effectiveness.

4. Staff Training and Awareness:

- We will conduct regular training sessions for key recovery personnel to ensure they are familiar with their roles and responsibilities in the event of a disaster.
- Additionally, we will raise awareness among all staff about the importance of disaster recovery planning and their role in supporting these efforts.

We are confident that these efforts will enhance our ability to recover from major disruptions to the District's information technology operations and minimize their long-term impact.

Response to Audit Finding 6: Information Technology Risk Assessment

The District acknowledges the findings and recommendations concerning the absence of a formal Information Technology Risk Assessment. The District currently employs a variety of methods to mitigate against threats and vulnerabilities, including:

- Monthly vulnerability scans on the district's public IP subnet, performed by both CISA and the district's insurance provider.
- A cloud-based security solution providing advanced threat detection and DNS security.

P.O. BOX 2118 · 200 NORTH CLARA AVE
DELAND, FL 32720
(386) 734-7190 · (386) 255-6475
An Equal Opportunity Employer

- An on-premises next-generation firewall with integrated threat intelligence and protection.
- An enterprise endpoint security platform providing real-time threat detection for both internal and external risks.
- Select ITS staff regularly receive cyber threat intelligence emails from CISA, ISAC, and the cybercrime office of the FDLE.

Corrective Actions Implemented and Planned:

1. Current Status

- While we have been conducting the various aforementioned risk assessment efforts, we acknowledge that these efforts need to be better documented and more comprehensively planned. This will ensure that all areas of risk are thoroughly assessed and managed.

2. Utilization of Frameworks

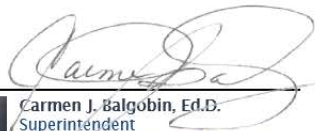
- We will continue to utilize established risk assessment frameworks such as NIST or CIS Controls to identify potential threats and their impact on critical data and operations so we can prioritize mitigation strategies effectively.

3. Documentation and Review

- All findings from the risk assessments will be documented, and a comprehensive risk management plan will be developed. This plan will include measures to mitigate identified risks and will outline the process for formally accepting residual risks where appropriate.

We recognize that threats and vulnerabilities are continuing to increase and evolve. In response, the District will engage a third-party provider to perform a comprehensive risk assessment within the 2025-2026 school year. This assessment will identify potential threats, vulnerabilities, and associated risks across the district's systems and policies. Based on the results, we will prioritize remediation actions according to severity and implement appropriate controls to mitigate risks. Any residual or accepted risks by the district will be documented accordingly.

Sincerely,




Carmen J. Balgobin, Ed.D.
 Superintendent
 Volusia County School District
 200 N. Clara Ave. | DeLand, FL 32720
 (386) 734-7190 ext. 20210
 Fax: 386-734-2842



P.O. BOX 2118 · 200 NORTH CLARA AVE
 DELAND, FL 32720
 (386) 734-7190 · (386) 255-6475
 An Equal Opportunity Employer