ARIZONA Auditor General
Making a Positive Difference

Coconino Association for Vocations, Industry and Technology
Initial Follow-Up Report

The June 2023 Coconino Association for Vocations, Industry and Technology performance audit found that the District did not take timely disciplinary action for repeated credit card misuse, lacked key outcome data demonstrating how the $1.9 million it spent in fiscal year 2021 effectively prepared students for high-need occupations, and put sensitive information at risk by not complying with important IT requirements and standards. We made 9 recommendations to the District, and its status in implementing the recommendations is as follows:

Status of 9 recommendations

Implemented	4
In process	2
Not implemented	**3**

We will conduct a 24-month followup with the District on the status of the recommendations that have not yet been implemented.

Finding 1: During a nearly 4-year period, former coordinator and their family member used District credit card for numerous personal purchases while superintendent did not take timely disciplinary actions

1. The District should ensure its employees comply with District policies and USFR requirements by enforcing existing District policies and cardholder agreements for District card usage. Actions the District should take include disallowing personal purchases, and taking timely, appropriate disciplinary action for noncompliance with card policies, such as recovering public monies; revoking card privileges; and termination.

   Not implemented—In December 2022, the District's governing board (Board) reviewed and approved credit card procedures that included disciplinary actions for employees for noncompliance. However, the District has not ensured that its employees complied with District policies and USFR requirements for using credit cards. Specifically, although our review of the District's 6 credit card purchases made in December 2023 did not identify any instances of misuse, employees did not prepare a requisition or receive preapproval for 4 of the 6 purchases as required by the District's credit card policies and procedures. We will review the District's adherence to the Board-approved policies and USFR requirements involving credit card purchasing and credit card misuse at the 24-month followup.

2. The District should ensure its employees comply with District policies and USFR requirements by continuing to implement and adhere to the credit card procedures the Board reviewed and approved in December 2022.

   Not implemented—As stated in recommendation 1, our review found that District staff have not consistently adhered to the District's updated credit card procedures approved by the Board in December 2022. We will review the District's adherence to the Board-approved policies and USFR requirements involving credit card purchasing and credit card misuse at the 24-month followup.

3. The District should ensure its employees comply with District policies and USFR requirements by developing and providing periodic training to its employees on District card policies and procedures, USFR requirements, and the appropriate disciplinary actions to be taken when improper use is identified.

   Not implemented—In July 2023, the District developed and provided training to its employees on District credit card policies and procedures, including the appropriate disciplinary actions to be taken when improper card use is identified. However, as previously discussed, our review of December 2023 purchases found that District cardholders were not consistently following District policies and procedures, despite having been trained in proper credit card usage, indicating that the District's training has not been effective or may need to be updated. We will review the District's efforts to implement this recommendation at the 24-month followup.

Finding 2: District's lack of key outcome data prevents it from demonstrating how the $1.9 million it spent on programs in fiscal year 2021 effectively prepared students for high-need occupations

4. The District should develop and implement consistent data collection protocols for all central and satellite career and technical education (CTE) programs. This includes collecting and validating complete data, such as data related to student certifications earned and job placements, as well as developing a process to track all outcome data as required by A.R.S. §§15-781, 15-391,15-393(L)(10)(b), and the Quality and Compliance Monitoring Document.

   Implementation in process—The District has begun taking steps to develop and implement consistent data collection protocols across its central and satellite CTE programs. Specifically, in September 2023 and January 2024, the District hosted meetings during which District and member district staff shared techniques and best practices for data collection and reporting. According to the District, District staff has also met individually with each member district to evaluate their progress in tracking relevant or required career and technical education district (CTED) data, including student enrollment and student outcomes, such as job placement and certification data. Additionally, the District developed enrollment and student outcome data collection forms and has distributed these forms to member districts. District officials indicated that all member districts are required to complete and submit these forms to the District beginning in May 2024 and annually thereafter. Although the District has taken some steps to ensure member districts consistently collect and report outcome data, the District reported that it has not yet developed protocols or plans for validating any data collected. We will review the District's data collection and validation efforts at the 24-month followup.

5. The District should analyze central and satellite CTE program outcome data to evaluate the effectiveness of its CTE programs in preparing students for high-need occupations and to support the investment of any public monies.

   Implementation in process—As stated in recommendation 4, the District has begun developing a process for collecting student outcome data to ensure consistency across the member districts and evaluate whether its CTE programs are effective and the best use of public monies. Additionally, in fiscal year 2024, the District analyzed student outcome data it previously collected to identify trends and modify the programs it offered for fiscal year 2025. In February 2024, the Board voted to discontinue 2 central programs based on negative trends it identified in student outcomes such as fewer certifications earned, technical skills examinations attempted or passed, and job placements secured.[1] In April 2024, the Board voted to discontinue funding 1 satellite CTE program based on similar data collected and reported between fiscal years 2019 and 2024.[2] Since the District is still in the process of collecting the outcome data needed to consistently evaluate its CTE programs, we will continue to assess the District's efforts to implement this recommendation at the 24-month followup.

[1] The Board voted to discontinue offering the Pre-Health Careers and Business Management programs provided by Coconino Community College for fiscal year 2025.

[2] The Board voted to discontinue funding Flagstaff Unified School District's Fashion Design and Operations program for fiscal year 2025.

Finding 3: District emailed unencrypted, sensitive information, and employees improperly shared login credentials, which were then stored in an unprotected document, increasing the risk of security breaches and fraud

6. The District should determine what type of information being shared with its accounting and business operations vendor is sensitive, personally identifiable information and should ensure that it only shares this information through secure means, such as through encrypted emails.

   Implemented at 6 months—In November 2023, the District's Board reviewed and approved data policies and procedures that identified what type of information being shared with its accounting and business operations vendor was sensitive, personally identifiable information. Additionally, according to the District's policy, sensitive information can no longer be shared through email and must be shared through secure means. Based on our review of the District's processes for data sharing, the District has implemented systems to securely share sensitive, personally identifiable information.

7. The District should continue developing and implementing written policies and procedures for securing sensitive, personally identifiable information to be shared with its accounting and business operations vendor to reduce the risk of unauthorized access to sensitive information or a security breach.

   Implemented at 6 months—As stated in recommendation 6, the District's Board reviewed and approved data policies and procedures in November 2023 that identified sensitive, personally identifiable information and required District staff to share sensitive, personally identifiable information with its accounting and business operations vendor only through secure means.

8. The District should identify District accounts with access to sensitive information, immediately reset passwords for the accounts, and keep the password credentials confidential.

   Implemented at 6 months—The District identified District accounts with access to sensitive information and required the associated account users to reset their passwords. Additionally, District officials reported that the District has kept the password credentials confidential by deleting the unprotected password computer document in November 2022 and by prohibiting password sharing, as stated in the District's Board-approved data policies and procedures.

9. The District should discontinue its practices of requiring employees to share passwords with the business office and storing passwords in an unprotected computer document, and should instead use more secure alternatives, such as creating administrator accounts, which could be used to reset terminated employee passwords when needed.

   Implemented at 6 months—As previously discussed, the District discontinued its practices of requiring employees to share passwords with the business office and deleted the unprotected password computer document in November 2022. Additionally, the District created system administrator accounts to enable designated staff to perform administrative duties within the District's systems. Based on our review of the District's system administrators, the District assigned administrator-level access consistent with credible industry standards.