Heber-Overgaard Schools

"Home of the Mustangs"

P.O. Box 547 Heber, Arizona 85928

Phone 928-535-4622 Fax 928-535-5146

www.heberovergaardschools.org

December 21, 2023

Walker & Armstrong LLP
1850 N. Central Ave., Ste 400
Phoenix, AZ 85004

To Whom It May Concern:

The Heber-Overgaard USD has received and reviewed the FY 20-21 / 21-22 / 22-23 Performance Audit Report. We would like to thank everyone on the audit team for their hard work and professionalism through this process.

After reviewing and discussing the audit findings and their recommendations we have addressed each area individually and have developed strategies and protocols moving forward. We believe these strategies will allow our district to enhance our performance and be more responsible as a school district that is entrusted to be fiscally responsible and to educate the wonderful students of our communities.

Please find attached the District's response to each finding and recommendation.

Respectfully,

Ron Tenney
Superintendent
Heber-Overgaard USD
Ph.: 928-535-4622
Email: *ron.tenney@h-oschools.org*

Finding 1: District lacked important internal controls, putting public monies at an increased risk for unauthorized purchases and fraud and potentially compromising student safety and sensitive personnel information

Recommendation 1: Develop and implement procedures to ensure the District obtains and documents appropriate approvals in advance of making purchases, as required by the USFR and District policy

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will review and update our procedures to be in compliance with USFR and District policy.

Recommendation 2: Develop and implement procedures to ensure employees and board members complete conflict-of-interest disclosure forms upon hire or the beginning of their term and annually thereafter in accordance with District policy.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: For the audit years reviewed, we only gave, forms to staff that attend orientation. FY23-24 we changed this procedure to include any employee that receives a paycheck. Policy for board member conflict of interest will be updated.

Recommendation 3: Review completed conflict-of-interest disclosure forms timely to identify and communicate conflicts of interest to the appropriate personnel to ensure the District takes action to remediate disclosed conflicts of interest to comply with District policies and State conflict-of-interest laws.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Recommendation 4: Develop and implement a process to ensure that all required personnel have a valid fingerprint clearance card, including:

Recommendation 4a: Maintaining documentation to support that all employees have fingerprint clearance cards if they are statutorily required to have one

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: District will use School ERP software to track all fingerprint clearance cards under the certification information. HR will review the list during Summer and Winter break to send out notifications to staff. HR will keep a list and verify all updated renewals as they come in. As well as identify those that have failed to renew.

Recommendation 4b: Monitoring and regularly reviewing employees' fingerprint clearance cards to confirm their validity

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Recommendation 5: Secure and retain personnel files in accordance with applicable document retention schedules.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Recommendation 6: Develop and implement a process for appropriately providing personnel records to terminated employees and require training for responsible employees regarding the process.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Oversight on the transportation director part. Procedure put into place- Transportation director will make copies of the transportation file for staff that request it and keep the original copy for district records.

Recommendation 7: Develop and implement policies and procedures for monitoring and reviewing usage logs for all District vehicles that includes ensuring vehicles are only used for an authorized purpose.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: For vehicles with a District Vehicle Authorization Form monthly logs will be turned into the transportation department. We have assigned an employee to physically verify mileage for all white fleet vehicles in the yard each day. This information is then verified and logged on a monthly spreadsheet maintained by the transportation director. Inventory for transportation supplies will be submitted yearly.

Finding 2: Districts excessive access to sensitive computerized data and other IT deficiencies increased the risk of unauthorized access to sensitive information, errors, fraud, and data loss

Recommendation 8: Implement and enforce strong password requirements that align with credible industry standards to decrease the risk of unauthorized persons gaining access to sensitive District information and disrupting operations.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: ALL critical district password control systems have been aligned with credible industry standards. Two-factor authentication has been implemented since our audit.

Recommendation 9: Develop and implement policies and procedures to review the District’s password standards against industry password standards at least annually.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Each year during the Summer months administration along with IT will review the district password standards to verify conformance to the industry password standards. Any changes will be implemented before all staff returns for the following school year.

Recommendation 10: Protect its sensitive computerized data by limiting users' access in the accounting system to only those accounting system functions needed to perform their job duties, including removing business office employee's administrator-level access.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We have cleaned up all the old staff accounts and are terminating access upon separation with the district. We have reviewed and adjusted all account access.

Recommendation 11: Develop and implement written policies and procedures to assign and periodically review accounting system access for employee accounts to ensure they have access to only those accounting system functions needed to perform their job duties. If separation of duties is not feasible due to a limited number of personnel, the District should implement other controls such as a process for a supervisor to regularly review system logs, balancing reports, and other relevant indicators, as required by the USFR.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will review all accounts during the Summer break and Winter break to verify access and responsibilities. Any updates will be made and notifications emailed out before staff returns to work.

Recommendation 12: Immediately disable or remove all network accounts associated with terminated employees.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Payroll will submit a ticket to IT with termination date. Checklists with all possible accounts will be reviewed before termination and IT will remove all access from any and all accounts within USFR guidelines.

Recommendation 13: Evaluate and document whether terminated employees accessed the District's network after their employment ended, such as unauthorized activities or changes that may have occurred as a result of potential improper access, and remedy any identified effects.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Any employee that has been terminated or resigned will have their account access removed immediately. The replacement or responsible employee will immediately be identified and all pertinent information will be transitioned. All transitioned accounts will be reviewed during Summer and Winter Break and removed.

Recommendation 14: Establish written policies and procedures to ensure that terminated employees' network access is promptly removed.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Payroll will submit a ticket to IT with termination date. Checklists with all possible accounts will be reviewed before termination and IT will remove all access from any and all accounts within USFR guidelines.

Recommendation 15: Develop and implement an IT contingency plan that meets USFR requirements and credible industry standards and test the plan at least annually to identify and remedy any deficiencies and document the test results.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will revamp our contingency plan within USFR guidelines. Training will be implemented for all new employees upon hire.

Recommendation 16: Restrict physical access to its IT server room so that only appropriate personnel have access.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: The IT server room will be re-keyed. A camera has been installed in the server room since our audit.

Recommendation 17: Develop and implement a written policy for distributing, tracking, and collecting keys that requires employees to sign an agreement outlining their responsibilities and that would allow the District to account for all keys.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We do have a physical tracking system, but failed to include the server rack keys. The key agreement has been updated to include all policies/procedures.

Recommendation 18: Conduct a physical inventory to determine and document the number of keys that exist and who has access to IT areas.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: An inventory has been done and all server rack keys have been identified and added to our key agreement.

Recommendation 19: Perform regular inspections of IT areas for maintenance needs to protect property and data.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: We will add an inspection of the server room and all network switch rooms to our Summer and Winter break duties and responsibilities list.

Recommendation 20: Develop comprehensive IT security policies and procedures in alignment with USFR requirements, and ensure they are consistently communicated to and implemented by staff to address the identified deficiencies and discrepancies in current operations.

District Response: The finding is agreed to, and the audit recommendation will be implemented.

Response explanation: Our IT Procedures will be revised and updated to comply with USFR guidelines.