



DEBRA K. DAVENPORT, CPA
AUDITOR GENERAL

STATE OF ARIZONA
OFFICE OF THE
AUDITOR GENERAL

MELANIE M. CHESNEY
DEPUTY AUDITOR GENERAL

June 6, 2013

The Honorable Chester Crandell, Chair
Joint Legislative Audit Committee

The Honorable John Allen, Vice Chair
Joint Legislative Audit Committee

Dear Senator Crandell and Representative Allen:

Our Office has recently completed a 24-month followup of the Antelope Union High School District's implementation status for the 7 audit recommendations presented in the performance audit report released in June 2011. As the enclosed grid indicates:

- 5 recommendations have been implemented, and
- 2 recommendations are in the process of being implemented.

Unless otherwise directed by the Joint Legislative Audit Committee, this report concludes our follow-up work on the District's efforts to implement the recommendations resulting from the June 2011 performance audit.

Sincerely,

Ross Ehrick, CPA
Director, Division of School Audits

RE:bl
Enclosure

cc: Dr. Andrew Smith, Superintendent
Governing Board
Antelope Union High School District

ANTELOPE UNION HIGH SCHOOL DISTRICT

Auditor General Performance Audit Report Issued June 2011 24-Month Follow-Up Report

Recommendation	Status/Additional Explanation
FINDING 1: District operates efficiently with most costs lower than peer districts'	
No recommendations	
FINDING 2: District lacks sufficient IT controls to adequately protect sensitive information	
1. The District should implement stronger password controls, requiring its employees to create more secure passwords and to periodically change those passwords.	Implemented at 6 months
2. The District should establish written policies and procedures for reviewing and monitoring user activity to determine whether any unauthorized activity or changes to critical applications or systems has occurred.	Implementation in process The District and the vendor that manages its systems and network have established a draft written agreement that addresses reviewing for unauthorized activity or changes to critical applications or systems. The District is working with the vendor to finalize the agreement.
3. The District should create a formal process for disabling unused network connection outlets on district walls.	Implemented at 12 months
4. The District should work with its IT vendor to establish written policies and procedures to address adding and deleting access to systems, including procedures to remove accounts when an employee leaves district employment.	Implemented at 24 months
5. The District should establish written agreements with its IT service providers that outline each party's responsibilities for its network, student information system, and accounting system.	Implementation in process The District and the vendor that manages its systems and network have established a draft written agreement that outlines each party's responsibilities for the District's network and systems. The District is working with the vendor to finalize the agreement.
6. The District should create a formal disaster recovery plan and test it periodically to identify and remedy deficiencies. Additionally, backup tapes should be stored in a secure offsite location.	Implemented at 12 months

Recommendation**Status/Additional Explanation****OTHER FINDINGS: District did not conduct random drug and alcohol tests**

1. The District should ensure that it conducts all required random drug and alcohol testing as specified in the *Minimum Standards*.

Implemented at 6 months