Subject: COVID-19 internal controls guidance

Arizona Auditor General

The COVID-19 virus pandemic has caused many districts to change their daily operating procedures and provide online educational opportunities to comply with the State and federal social distancing guidelines. As districts establish controls in this new online environment, they should continue to follow their policies and procedures to ensure that adequate internal controls remain in place to protect taxpayer dollars, district data, and student and staff safety.

Although the methods of performing work may have changed with more staff working remotely, it is important to remember that the *Uniform System of Financial Records* (USFR) requirements still apply. Districts should maintain an effective internal control environment to help them avoid any occurrences of fraud, theft, or misuse in this time of uncertainty and change. For example, districts should require approved purchase orders prior to ordering goods or services and approved expenditure documentation prior to issuing payments.

For **any** temporary modifications to normal operating procedures, districts should:

- Ensure that adequate separation of responsibilities remain in place.
- Document any temporary modifications to operating procedures and notify employees about the new procedures.
- Document when and why USFR requirements are not able to be met (if necessary) and any compensating controls that are put in place.

Districts should review the Fraud Prevention Alerts on our website with information on Phishing Scam Emails and Ransomware and instruct their employees on what to do if they receive a suspicious email because there has been a surge in reported COVID-19-themed phishing emails and ransomware schemes that threaten district resources. These emails may include:

- Subject lines that indicate there is important information included or action required, such as "Coronavirus-Shipping information," "CDC-Corona virus outbreak in your city," "Stimulus payments," "Corona Virus maps," or "Donate Now."
- Suspicious language, misspelled words, or poor grammar.
- Requests for private information or payments made without following established procedures.

Districts should remind employees to watch for and report suspicious email and be skeptical about clicking on links or providing any information to the email sender. As staff work remotely, they should follow revised expenditure processing policies and procedures districts have in place, which should continue to require adequate documentation and approval for any expenditure request.

Further, the Arizona Attorney General issued guidance relating to Arizona's Open Meeting Law and COVID-19 on March 13, 2020. Districts should review this guidance as it includes suggestions for holding remote public meetings through technological means, such as conference calls, webinars, or video conferencing tools.

Finally, as districts use video conferencing tools to hold meetings or provide online instruction, they should ensure their policies and procedures address physical and information security. Districts should review the FBI's recently issued warning about teleconference security and ensure platforms and software used for online conferencing protect students, staff, and district data.

If you have any questions, please contact Cris Cable or Megan Smith, Accountability Services Managers, at asd@azauditor.gov or (602) 977-2796.