September 2016

**Nicole Galloway, CPA**
**Missouri State Auditor**

# CITIZENS SUMMARY

## Findings in the Cyber Aware School Audit of the Orchard Farm R-V School District

### Background

The Orchard Farm R-V School District's Student Data Governance Audit was completed as part of the Cyber Aware School Audits Initiative. These audits are designed to assess the effectiveness of privacy and security controls with a focus on identifying practices to improve the security of information school districts have on students and their families. The district uses a student information system (SIS) to maintain student data and to track and monitor academic progress. The SIS maintains private and confidential data, such as assessment test scores and other sensitive data. Additional systems and applications that maintain data are used for administrative functions and to enhance student productivity and classroom collaboration. The district relies extensively on computerized systems to support its educational and mission-related operations and on information security controls to protect the sensitive data residing on those systems. Auditors identified areas where improvements are needed but also found the district has developed certain controls to establish a safe environment for using technology, including promoting online safety, security, and confidentiality.

### Data Governance

The district has not completed establishing a comprehensive data governance program, a critical task for any educational organization. A comprehensive program is necessary to ensure the confidentiality, integrity, availability, and quality of data. Without a formal program, the district cannot ensure that personally identifiable information (PII) is adequately protected and safe from unauthorized access, misuse, or inadvertent disclosure.

### Review of User Access

The district does not perform periodic reviews of users' access to data to ensure access remains appropriate and aligned with job duties. As users' work assignments and job responsibilities change, access rights to systems may be added, changed, or removed. Over time, users can accumulate access rights that are no longer necessary, increasing the risk of inappropriate access to data.

### Security Controls

The district has not implemented or documented policies and procedures for certain security controls, leaving district technology assets, including PII, at risk of inappropriate access, use, and disclosure. The district has not documented policies and procedures to identify the types of security events to be logged and monitored. The district has not documented policies and procedures for certain security controls. Without documented and approved policies and procedures, management may not have assurance that control activities are appropriate and properly applied.

### Continuity Planning

The district has not completed or formally tested its continuity plan. District personnel created a continuity plan in 2013; held discussions to add key contacts and vendors to the plan; and updated the plan in July 2016, indicating the district has made progress. However, the plan needs to be completed and formally tested. Without a tested and functional continuity plan, management has limited assurance the organization's business functions and computer processing can be sustained during or promptly resumed after a disruptive incident.

## Vendor Controls

The district has not established a process for ensuring software acquired or outsourced from information technology vendors complies with data security principles, and the district's contract for a key system does not fully define expectations over securing and accessing district data. Data maintained by the system is hosted locally by the district. However, data is also routinely backed up to the vendor site. Without an effective process for monitoring and managing risk of software acquisition or outsourcing, and without fully defining expectations over district data, the district has less assurance in a vendor's ability to deliver services effectively, securely, and reliably and to ensure that services meet current and future data privacy and security needs.

Because of the nature of this report, no overall rating is provided.

**All reports are available on our Web site: auditor.mo.gov**