Carmel CSD Corrective Action Plan for Internal Control Risk Assessment for 2020-2021 (REVISED)

Area: Accounting, Reporting and Information Technology:

Auditor's Finding:

a.) Based on discussions with Technology personnel, it does not appear that the District has a formal process in place related to performing phishing prevention exercises. Phishing is the attempt to acquire sensitive information such as usernames, passwords, financial details, or other personal information, often for malicious reasons. Successful phishing campaigns are a leading cause of data breaches and other events that compromise an organization's network. Phishing is also the delivery mechanism of choice for ransomware and other malware. Conducting phishing prevention exercises, through sending test emails to staff, can be useful in assessing the effectiveness of the required annual awareness training and reinforcing its importance with personnel.

b.) Given the necessity for remote learning during the current COVID-19 pandemic, the District has distributed devices to virtually all of its students. This represents a significant increase in the number of District devices that are in service, all of which now remain with the students for both in-school and remote instruction. At this time, the District has not implemented a voluntary insurance program that can help students and the District manage the risk associated with lost, stolen, or damaged devices.

Auditor's Recommendation:

a.) We encourage the District to consider developing a formal phishing prevention program that can be used to evaluate the effectiveness of its cybersecurity awareness training efforts. The District should also consider potential disciplinary responses for personnel who fail these exercises, including warnings, remedial training, or further reprimands for employees who fail multiple exercises.

b.) Although the District has not yet experienced significant costs related to lost or damaged devices, we encourage the District to evaluate whether implementing an optional insurance program for students could help both the District and students/families in managing the risk of increased repair and replacement costs associated with the increased number of devices in service.

District's Corrective Action:

a.) The District has implemented the use the Global Compliance Network to address the formal training required to mitigate the risks due to phishing and Educational Law 2-D. In the 2022-2023 school year, the district will be implementing a program called Info Sec. This program addresses the need to build safe email behavior by employees by providing online training videos and activities. The district then can conduct occasional mock phishing attacks to help users learn how to recognize and report phishing attacks. The District will also continue to work with the LHRIC Data Protection Service to stay abreast of current best practices for cyber security including the prevention of phishing attacks.

b.) The District has started the process of researching alternative insurance programs as well as repair programs and will evaluate the cost/benefit of implementing such programs to determine if the cost of insurance is more then or less then annual repair costs without insurance.
The district has also implemented a fee schedule for damaged and lost devices and an online payment system for parents to remit payment.

Implementation Date(s):

a.) September 2021 through June 30, 2022
b.) September 2021 through June 30, 2022

Person Responsible for Implementation:

Assistant Superintendent for Pupil Personnel Services and Technology
CIO, Director of Data Management