Remote Work

Internal Audit Report

November 1, 2020

Orange County Public Schools
Internal Audit

Linda J. Lindsey, CPA, CGAP, School Board Internal Auditor
Alpa Vyas, Senior Internal Auditor

Table of Contents

BACKGROUND:

While employees worked from non-district facilities prior to the current pandemic, these instances were generally limited in scope and duration and usually involved administrative employees. Beginning with the stay-at-home order in March, 2020, most employees worked remotely, and even today we have a significant number of employees who continue to do so.

When the pandemic struck, we re-evaluated our audit risk assessment and the audit plan and placed emphasis on new or increased risks that came with it. Remote work is an increased risk area because large numbers of employees were asked to perform their work away from district facilities.

OBJECTIVE, SCOPE AND METHODOLOGY:

Objective

The objective of this audit was to evaluate potential data risks to the district associated with remote work by employees during the COVID-19 pandemic.

We evaluated risks associated with remote work.

Scope

The scope of the audit covered the period from March through August, 2020.

Methodology

We reviewed existing School Board Policies, Management Directives and IT standards and guidelines.

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors and included such procedures as deemed necessary to provide reasonable assurance regarding the audit objective. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. No material deficiencies were noted in this audit. We also offer suggestions to improve controls or operational efficiency and effectiveness.

RESULTS & RECOMMENDATIONS:

Overall Conclusion:

Our overall conclusion is that the district should provide guidance that addresses data security when employees work at locations outside OCPS facilities. ***Significant Risk***

Best Practice:

Remote work guidance addressing data security would help to inform, guide, and communicate to employees the district's expectation of protection of data and assets when working outside of OCPS locations. Training to all employees on such policies is critical to success. Vulnerability of data is one of the highest risks during the COVID-19 pandemic as remote work has become more common.

Effective remote work guidelines would address data security matters such as strong home Wi-Fi passwords, restrictions on the use of public Wi-Fi, use of encryption, restrictions on use of personal devices for district work, access only through OCPS Virtual Private Network (VPN), strong network security, physical security of work devices, and restrictions on accessing personal emails, spam emails, unapproved software, and unsecured websites on district devices.

Audit Results:

The district has established data security policies and guidelines. However, these do not address data security/protection of data when employees work remotely outside OCPS buildings such as in homes, airports, hotels, or other public places.

When employees were asked to work remotely, they each adapted as best they could in the circumstances. Some had no home internet and had to work in places with unsecured public Wi-Fi. Although they could not access the district's network without going through the VPN,

Remote work guidelines should address:

- *Strength of home Wi-Fi passwords*
- *Restrictions on use of public Wi-Fi*
- *Use of encryption*
- *Restrictions on use of personal devices*
- *Accessing the OCPS network via VPN*
- *Physical security of work devices*
- *Restrictions on use of work devices*

Existing data security policies do not address remote work.

they could send and receive district email, including emails with attachments, and work on files outside of the network. They could also log in to cloud based systems like School Funds Online without going through the district network. Some downloaded district financial and student records on their devices or on external media in order to be productive.

Recommendation:

The district should issue remote work guidance addressing data security/protection of data and provide training on the policy.

MEMORANDUM

ITS
Chief Information Office

Date: December 8, 2020

To: Linda Lindsey, School Board Internal Auditor

From: Robert Curran, Chief Information Officer

Subject: Management Response to Remote Work Preliminary & Tentative Draft Report

Recommendation: The district should issue remote work guidance addressing data security/protection of data and provide training on the policy.

Management Response: ITS agrees that remote work guidelines need to be established. ITS Information Security will head up creating the document with input from other areas that can be sent to OCPS Administrators for dissemination. Anticipated completion of document is March 1, 2021.