Maricopa County Office of Enterprise Technology
Audit of Remote Access Management and Security
By Maricopa County Internal Audit
December 2022

Why This Audit Is Important

Maricopa County leadership offered remote work options to much of the County's workforce during the pandemic so that employees could provide services to county residents in a safe manner. When the pandemic subsided, the County adopted a hybrid model to support a blend of in-office and remote work.

Security risks are inherently elevated as employees access sensitive data remotely using non-county Wi-Fi connections and devices. Strong IT security, policies, and employee awareness training are necessary to defend against security and data breaches.

We performed this audit to assess the status of the County's controls and related security procedures for remote access to sensitive data. Our review focused on departments supported by the Office of Enterprise Technology (OET) and included a review of current practices and countywide training in comparison to nationally recognized best practices and county policies. For security purposes, some details are withheld from this report.

Key Results

- Device patching improvements are underway to improve remote work security.
- Employee IT security training can be improved by including additional information about security threats faced by remote workers.

All key findings requiring corrective action were addressed through agreed-upon management action plans.

What We Audited

Following is a summary of work performed and recommendations. The responses were approved by Ed Winfield, Chief Information Officer, on December 2, 2022. We also communicated detailed observations and recommendations.

Security and Monitoring

Background: We reviewed nationally recognized best practices for securing remote work environments and compared them to OET's ongoing efforts. We also interviewed Information Security Division leadership to understand OET's processes for securing and monitoring devices and data used by remote workers.

Observations: We determined that the County follows most applicable best practices for securing remote work environments. We noted that some technology tools and processes are

not yet fully implemented to address device patch failures in a timely manner. Stopgap measures are needed until these tools and processes are in place.

Recommendation to OET	Response
Review the current patching process for interim improvements until technology tools and resources are fully implemented.	Concur – in progress 1. Selection and Implementation of ITAM (in progress) 2. Set up Monthly InfoSec/BEM/EDCS meeting to discuss systems at risk (complete) Target Date: 3/30/2023

In addition, OET has installed network monitoring tools to identify when department data is transferred from the County network to an external location. There is a risk that sensitive data can be stored in an insecure location (e.g., non-OET supported cloud storage). Data security can be strengthened by implementing data classification policies and processes so that OET can identify sensitive data and implement appropriate safeguards. OET's draft data classification policy is in the final stages of approval.

Recommendation to OET	Response
Until the data classification policy and processes are in place to mitigate data loss risks, interim measures are needed to assess whether department data transferred from the network may pose a security risk.	Concur – will implement with modifications 1. Complete implementation of DLP Policies in Netskope 2. Complete SOPs for InfoSec Analysts to effectively identify and communicate policy violations 3. Continue to educate and publicize the importance of good data management practices including the transfer of data outside the County. Target Date: 3/30/2023

Policies and Training

Background: We reviewed countywide IT policies and required security trainings to determine if they provided sufficient guidance to employees on protecting sensitive data while working remotely. We also surveyed department leaders to better understand existing practices and controls for remote worker access to sensitive department data.

Observations: County policies adequately address most nationally recognized best practices for securing remote work. Employees are required to attend two online IT security trainings covering common security threats. However, the required training does not cover important security defenses for remote workers. We provided OET with the best practices and controls so that improvements can be made to policies and training.

Recommendation to OET	Response
Review the remote access controls highlighted by nationally recognized best practices to identify and implement policy and training improvements.	Concur – will implement Revise Policy Training content with MHR Employee Development Team Target Date: 6/30/2023

Our survey of department leaders identified some security awareness opportunities for remote workers. We partnered with OET to prepare a list of tips that can help remote workers reduce security threats. The Communications department published a summary of these tips as part of an awareness message for the October *Maricopa Currents* employee newsletter to coincide with Cybersecurity Awareness month.

Additional Information

This audit was authorized by the Maricopa County Board of Supervisors and was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing. This report is intended primarily for the Maricopa County Board of Supervisors. However, this report is a public record, and its distribution is not limited. If you have any questions about this report, please contact Mike McGee, Internal Audit Director, at 602-506-1585.