# Executive Summary

# Purpose

Robert A. Kalka Metropolitan Skyport enlisted the help of <<REGIONALS/FINALS-#>>’s penetration testing services to evaluate their corporate, customer user, transport train, and guest networks. This test was an assessment for vulnerabilities present in Robert A. Kalka Metropolitan Skyport’s networks. The penetration test occurred on 10/14/2023 and encompassed a singular workday.

This penetration test is designed to help Robert A. Kalka Metropolitan Skyport better secure its critical infrastructure. Our firm and RAKMS understand that protecting these systems has a direct impact on a customer’s safety and experience with the company. Throughout this engagement, our firm considered customer safety as the primary factor when conducting tests and assessing the criticality of vulnerabilities. It is of the utmost importance that the customer and their data are kept safe and secure to maintain Robert A. Kalka Metropolitan Skyport’s commitment to its customers.

Findings

Among the findings from our assessment, a few were particularly noteworthy due to their significant risk to Robert A. Kalka Metropolitan Skyport’s airport operations safety. The first of these is <<Finding 1 and details regarding how it affects business>>. The second, of which, is <<Finding 2 and details regarding how it affects business>>. A final finding that should be addressed is <<Finding 3 and details regarding how it affects business>>. Our firm wanted to highlight the listed vulnerabilities as the most important points of failure found during the engagement. We recommend remediating these vulnerabilities immediately to mitigate risk to airport operations safety and customer privacy. This will help protect the company from disruptions to business operations, damages to business reputation, and an erosion of trust between the business and the consumer.

While this test was designed to find system and business process vulnerabilities, it was also a test of the security posture of Robert A. Kalka Metropolitan Skyport’s Networks. Based on our testing, we found RAKMS excelled in the areas of <<AREA1, AREA2, AREA3>>. <<Details for Area 1 explaining why they did well>>. <<Details for Area 2 explaining why they did well>>. <<Details for Area 3 explaining why they did well>>. We commend the RAKMs staff for excelling in these areas of the business’ security posture.

Overall, our firm discovered <<NUMOFFINDINGS>> findings which contributed to unauthorized access of the Robert A. Kalka Metropolitan Skyport corporate, customer user, transport train, and guest networks. Our findings consisted of <<PERCENTCRIT>> Critical, <<PERCENTHIGH>> High, <<PERCENTMED>> Medium, <<PERCENTLOW>> Low, and <<PERCENTINFO>> Informational. Once the documented exploitable vulnerabilities are corrected, many of the attacks performed in the testing of the listed networks by our firm would be impossible to accomplish which will substantially lower the risk to airport operations safety, customer data, business technology service uptimes, and would increase the overall safety of the network while improving operating costs.

Compliance

Understanding that Robert A. Kalka Metropolitan Skyport falls under the TSA’s standards for safety and security compliance, the three highest priority standards requiring re-evaluation are the <<LISTOFCOMPLIANCEAREAS>> areas of security compliance. As understood by RAKMS, a failure to meet these standards can result in safety violations, legal fees and fines, reputational damage, loss of consumer trust, operational disruption, and more. Our firm recommends analyzing the following findings and correcting them and the vulnerabilities described earlier: <<FINDING1COMPLIANCE and details, etc.>>. Following the recommendations will assist RAKMS in maintaining security compliance standards and the business will improve the airport operations safety and information security posture critical to protecting consumer data.