Compliance Summary

TSA Security Directive 1580/82-2022-01 and TSA Security Directive 1582-21-01A

The Robert A. Kalka Metropolitan Skyport is an airport that deals with public transportation. Due to this, the Robert A. Kalka Metropolitan Skyport must adhere to Transportation Security Administration (TSA) security directives. TSA security directives are a set of mandatory measures that public transportation businesses must follow to ensure national security and public safety. Failure to adhere to security directives may result in penalties such as fines, additional security restrictions, or suspension of flights across the United States resulting in a loss of business and credibility. There are certain aspects of the security directives that are unable to be assessed through a standard penetration test.

References:

<https://www.tsa.gov/sites/default/files/sd-1580-82-2022-01.pdf>

<https://www.tsa.gov/sites/default/files/sd-1582-21-01a.pdf>

|  |  |  |  |
| --- | --- | --- | --- |
| TSA Security Directive Objectives | TSA Requirements | Compliance Violation Findings | |
| Implement strong access control measures | 1. Policy for secret authenticators resets, that include criteria when resets must occur | -  - | TCC013 TCC031 |
|  |  |  |  |
|  | 2. Defined mitigation measures for components  of Critical Cyber-Systems |  | |
|  |  |
|  |  |
|  |  |
|  | 3. Multi-factor authentication or other supplementary security control |  | |
|  |  |  | |
|  | 4. Managed access rights based on principles of least privilege |  | |
|  |  |  | |
|  |  |  | |
|  | 5. Regularly update schedule for review of existing domain trust relationship |  | |
|  |  |  | |
| Implement Continuous monitoring and detection policies | 6. Capabilities to defend against malicious email, block communications with suspected malicious machines, control impact of known or suspected malicious web domains, block and prevent unauthorized codes from executing, and monitor and/or block connections from malicious command and control servers |  | |
|  |  |  | |
|  |  |  | |
|  | 7. Procedures to audit unauthorized access to internet domains and addresses, document and audit communications between systems, identify and respond to execution of unauthorized code, and implement capabilities to define, prioritize, and drive standardized incident response activities. |  | |
|  |  |  | |
|  | 8. Logging policies that require continuous collection and analysis of data for potential intrusions, and ensure that data is maintained for sufficient periods |  | |
|  |
|  |
|  |  |  | |
|  |  |  | |
|  | 9. Measures or controls to ensure industrial control systems can be isolated |  | |
| Reduce the risk of exploitation of unpatched systems | 10. Patch management strategy that ensures critical system security patches are up to date |  | |
|  |  |  | |
|  |  |  | |
|  | 11. If patches result in severe degradation of operation capability, must have sufficient mitigations that address the risk |  | |
| Develop a Cybersecurity Assessment program for proactively assessing and auditing Cybersecurity measures | 12. The owner/operator must develop a cybersecurity assessment plan to ascertain the effectiveness of cybersecurity measures and to identify vulnerabilities |  | |
|  |  |  | |
|  |  |  | |
| Designate a Cybersecurity Coordinator | 13. Coordinator who is always available to coordinate the implementation of cybersecurity practices, and serve as a point of contact with TSA and CISA for cybersecurity-related matters | Not testable with a penetration test | |
|  |  |  | |
| Reporting Cybersecurity Incidents | 14. Owner/Operators are required to report cybersecurity incidents to CISA involving systems that the Owner/Operator has the responsibility to operate | Not testable with a penetration test | |
|  |  |  | |
|  |  |  | |
| Implement a Cybersecurity Incident Response Plan | 15. Prompt identification, isolation, and segregation of infected systems from uninfected systems |  | |
|  |  |  | |
|  |  |  | |
|  | 16. Secure backed-up data and measures to ensure the integrity of backed-up data |  | |
|  | 17. Identifies who is responsible for implementing the specific measures and any necessary resources needed |  | |
|  |  |  | |
|  | 18. Owner/Operator must conduct situational exercises to test the effectiveness of procedures, and personal responsible for implementing measures, no less than annually. |  | |
| Conduct Vulnerability Assessment | 19. Owners/Operators must conduct cybersecurity vulnerability assessments to identify cybersecurity gaps using a form provided by TSA. Form utilizes functions and categories found in the NIST Cybersecurity Guidance Framework. |  | |
|  |  |  | |
|  |  |  | |
|  | 20. Owners/Operators must identify remediation measures to address vulnerabilities and gaps identified in the assessment |  | |
|  | 21. Completed vulnerability assessment form and remediation plan must be submitted to TSA |  | |