Security Level Agreement

Between airlines

and

airline financial system

|  |  |
| --- | --- |
| **Date** |  |
| **Version** |  |
| **Key Points:** |  |

Table of Content:

[Introduction: 3](#_Toc162362058)

[1. Objective and Scope 3](#_Toc162362059)

[2. Service Availability 3](#_Toc162362060)

[2.1. Uptime Commitment: 3](#_Toc162362061)

[2.2. Maintenance Windows 3](#_Toc162362062)

[3. Security Measures 3](#_Toc162362063)

[3.1. Encryption and Masking: 3](#_Toc162362064)

[3.2. Network Security: 3](#_Toc162362065)

[3.3. Access Control: 3](#_Toc162362066)

[4. Incident Response 4](#_Toc162362067)

[4.1. Incident Response Plan: 4](#_Toc162362068)

[4.2. Notification Protocol: 4](#_Toc162362069)

[5. Data Integrity and Confidentiality 4](#_Toc162362070)

[5.1. Data Backup: 4](#_Toc162362071)

[5.2. Confidentiality Agreements: 4](#_Toc162362072)

[6. Performance Monitoring and Reporting 4](#_Toc162362073)

[6.1. Security Monitoring: 4](#_Toc162362074)

[6.2. Quarterly Security Reports: 4](#_Toc162362075)

[7. Log System, Access Logs, and Audit Trail 4](#_Toc162362076)

[7.1. Log System: 4](#_Toc162362077)

[7.2. Access Logs: 4](#_Toc162362078)

[7.3. Audit Trail: 4](#_Toc162362079)

[8. Audit and Compliance 5](#_Toc162362080)

[8.1. Annual Security Audits: 5](#_Toc162362081)

[8.2. Regulatory Compliance: 5](#_Toc162362082)

[9. Review and Amendment Process 5](#_Toc162362083)

[10. Penalties and Remedies 5](#_Toc162362084)

[11. Confidentiality 5](#_Toc162362085)

[12. Signatures 5](#_Toc162362086)

# Introduction:

This Security Level Agreement is entered into as of Mach of 2024, by and between Airline company Airlines, a leading airlines company headquartered in Syria (as the customer), and System Provider, a leading technology partner for the Travel Industry headquartered in India (as the system provider).

This Security Level Agreement specifies the security measures, protocols, and standards that the Provider, is committed to maintaining in the delivery of the Financial System to Airline company Airlines.

This document represents a binding agreement between Airline company Airlines and System Provider, ensuring a secure, reliable, and compliant financial system environment.

# 1. Objective and Scope

The primary objective of this Security Level Agreement is to determine the security framework within which the Provider will operate and maintain the System for Airline company. This includes determining the expectations for data security, system integrity, and confidentiality in line with industry best practices and regulatory requirements. The scope covers all software, hardware, and services provided as part of the System.

# 2. Service Availability

2.1. Uptime Commitment: The Provider guarantees a System uptime of 99.9%, excluding planned maintenance.

2.2. Maintenance Windows: Planned maintenance will be scheduled during the least impactful hours, communicated to the Airline at least 48 hours in advance, and not to exceed 12 hours per month.

# 3. Security Measures

3.1. Encryption and Masking: All data transmitted between the Airline and the System, as well as data stored within the System, will be secured using AES-256 encryption or higher standards. Additionally, sensitive information will undergo data masking to ensure further privacy and security, making it unreadable and inaccessible to unauthorized users both during transmission and storage.

3.2. Network Security: Deployment of firewalls, intrusion detection/prevention systems (IDS/IPS), and regular vulnerability scans to safeguard the System against unauthorized access and cyber threats.

3.3. Access Control: Implementation of strict access control measures including multi-factor authentication, role-based access control, and regular access reviews to ensure that only authorized personnel can access the System.

# 4. Incident Response

4.1. Incident Response Plan: The Provider maintains a comprehensive incident response plan, including immediate incident containment, eliminating of threats, recovery of operations, and post-incident analysis.

4.2. Notification Protocol: In the event of a security incident, Airline company staff will be notified within 24 hours, with ongoing updates as the situation evolves and a detailed report following the incident's resolution.

# 5. Data Integrity and Confidentiality

5.1. Data Backup: Regular, encrypted backups of all Airline company data by Airline company side, with the capability to restore operations swiftly in the event of data loss.

5.2. Confidentiality Agreements: All Provider personnel with access to Airline company data will have signed confidentiality agreements to protect sensitive information.

# 6. Performance Monitoring and Reporting

6.1. Security Monitoring: Continuous monitoring of the System for security threats, with the use of advanced security information and event management (SIEM) tools.

6.2. Quarterly Security Reports: Provision of detailed security reports to Airline company Management and concern parties every quarter, including incident logs, trends, and actionable insights.

# 7. Log System, Access Logs, and Audit Trail

7.1. Log System: The Provider will implement a log system that records all significant security events, including but not limited to user access, system changes, and security alerts.

7.2. Access Logs: Detailed logs regarding who accessed what data within the System will be maintained, ensuring traceability of all actions performed within the system.

7.3. Audit Trail: A comprehensive audit trail will be kept, documenting the sequence of authenticated user activities and system processes affecting data and system integrity. This includes actions taken by users, date and time stamps, and the impact of the action.

# 8. Audit and Compliance

8.1. Annual Security Audits: Conduct of annual security audits by a third-party auditor or by the audit authority in Airline company, with findings and recommendations shared with the company.

8.2. Regulatory Compliance: Assurance of compliance with applicable aviation and data protection regulations, including GDPR (General Data Protection Regulation – 2018), and any relevant aviation authority regulations.

# 9. Review and Amendment Process

9.1. This agreement is subject to review and renewal upon significant changes to the services, technology landscape, or regulatory environment.

9.2. Any amendments to this agreement must be mutually agreed upon in writing by both parties.

# 10. Penalties and Remedies

10.1. Failure to meet the agreed-upon service availability or a breach of security measures will incur penalties, including service credits and this to be determined later.

10.2. Repeated failures or breaches may trigger a re-evaluation of the agreement, leading to renegotiation or termination.

# 11. Confidentiality

Both parties commit to protecting the confidentiality of the information exchanged under this agreement, employing at least the same level of care as they use to protect their own confidential information, but no less than reasonable care.

# 12. Signatures

By signing below, both parties agree to the terms outlined in this Security Level Agreement and commit to uphold the security standards set forth to ensure the protection and integrity of Airline company’ data and financial transactions.

|  |  |
| --- | --- |
| **For Airline company: Name: Title: Date:** | **For System Provider: Name: Title: Date:** |