**A PROPOSED OFFERING OF BUS TICKETING AND BOOKING SYSTEM**

**FOR VICTORY LINER INC.**

A Project Proposal Presented to the

Faculty of Datamex College of Saint Adeline, Inc.

In Partial Fulfillment of the Requirements for the

Degree of Bachelor of Science in Information Technology

By:

Arellano, Romeo C.

Estigoy, Ron Kyrie

Flores, Joserey G.

Gadi, Susana

October 2025

**MAINTENANCE DOCUMENTATION**

**INTRODUCTION**

The Bus Ticketing and Booking System is created to simplify ticket reservations, scheduling, and passenger management. Passengers can book tickets online or at terminals. The system gives operators real-time schedules and manages payments safely.

Regular maintenance is essential to keep the system reliable, secure, and performing well. Without consistent maintenance, risks like data loss, downtime, or security gaps can disrupt operations.

**Maintenance includes:**

Software updates and patches

Bug identification and fixes

Security improvements, such as data encryption and access control

System optimizations and scalability improvements

**Maintenance Plan**

Our maintenance strategy ensures the system runs smoothly, stays secure, and can grow as needed. Types of maintenance include:

**Corrective Maintenance:** Fixing bugs like booking errors, failed transactions, or login issues.

**Adaptive Maintenance:** Updating APIs for payment gateways, adjusting to OS or browser updates, or following new transport regulations.

**Perfective Maintenance:** Improving system speed and adding features like seat selection or mobile notifications.

**Preventive Maintenance:** Regularly cleaning the database, monitoring performance, and conducting security audits.

**Maintenance Schedule**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Description** | **Responsible person** | **Frequency** | **Status** |
| Security Updates | Create full backups of th | Programmer | Weekly | Ongoing |
| Database Backup | update firewalls and SSL certificate | Programmer | Monthly | Scheduled |
| Security Updates | Resolve reported booking and payment issues | Programmer | Weekly | Pending |
| Bug Fixes | Monitor load times and optimize server usage | System analysts | Monthly | Scheduled |
| System Performance Check | Monitor load times and optimize server usage | System analysts | Weekly | Pending |
| User Feedback Review | Review and apply suggestions for improvements Quarterly | User | Monthly | Scheduled |

**Issue Tracking & Bug Reports**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Issue Id** | **Description** | **Severity** | **Reported By** | **Date reported** | **Status** |
| BUG001 | Login page does not loa | High | User A | 09/05/202 | Fixed |
| BUG002 | Payment gateway error | Critical | User B | 09/08/202 | Progress |
| BUG003 | Incorrect bus schedule show | Medium | User C | 09/12/2025 | Pending |
| BUG004 | Ticket PDF not generating | High | User D | 09/15/202 | Resolved |

**Backup & Recovery Plan**

**Backup Procedures**

**Frequency:**

Daily incremental backups and full backups every Sunday.

Storage Locations: Local server, cloud storage (AWS S3), and encrypted external drives.

**Recovery Steps**

1. Identify the failure, such as database corruption, server crash, or cyberattack.

2. Shut down the system to prevent further data loss.

3. Retrieve the latest verified backup from AWS S3.

4. Restore database and application services.

5. Verify system integrity by testing bookings and payment flow.

6. Resume operations.

**Technical Support Contact:**

IT Support Hotline: +63-XXX-XXX-XXXX

Email: support@busticketing.com

**Performance Monitoring**

|  |  |  |  |
| --- | --- | --- | --- |
| **Metric** | **Description** | **Threshold** | **Monitoring tool** |
| Server Uptime | System availability | 99.9% | AWS CloudWatc |
| Response Time | Page load speed | 2 secs | Google Lighthouse |
| Error Rate | Percentage of failed request | 1% | Log Analyze |
| Transaction Success Rate | Successful payments | 98% | Payment |

**| Metric | Description | Threshold | Monitoring Tool |**

**|--------------------------|----------------------------|------------|--------------------------|**

**| Server Uptime | System availability | 99.9% | AWS CloudWatch |**

**| Response Time | Page load speed | < 2 sec | Google Lighthouse |**

**| Error Rate | Percentage of failed requests | < 1% | Log Analyzer |**

**| Transaction Success Rate | Successful payments | > 98% | Payment Gateway Dashboard |**

**Security Measures**

Access Control: Role-based access for admin, operators, and users.

Authentication: Two-factor authentication (2FA) for admin accounts.

Encryption: All sensitive data, including passwords and payment details, is encrypted using AES-256.

Secure Communication: Enforced HTTPS with updated SSL and TLS certificates.

Regular Audits: Quarterly penetration testing and vulnerability scans.

**Documentation Updates**

Added recovery steps for failed payment transactions (09/10/2025).

Updated database schema documentation to include the new "Discount Codes" table (09/15/2025).

Revised system architecture diagram to show new cloud backup integration (09/20/2025).

**Conclusion & Recommendations**

Summary of Maintenance Tasks Completed

Throughout the maintenance period, several key activities were performed to ensure the smooth operation of the Bus Ticketing System. These included fixing reported bugs in ticket booking and seat allocation, optimizing page loading speed, updating security patches to protect user data, and conducting database cleanup to improve performance. Minor interface adjustments were also made to enhance user experience for both passengers and staff.

**Recommendations for Future Improvements**

To further strengthen the system, it is recommended to implement the following enhancements:

Introduce automated notifications for ticket confirmation, trip reminders, and schedule changes.

Add system monitoring tools to detect performance issues earlier and reduce downtime.

Enhance reporting features for easier tracking of sales, routes, and passenger data.

Improve mobile usability by optimizing the interface for different screen sizes and devices.

Schedule regular security audits to ensure continued protection of personal and payment information.