**A PROPOSED OFFERING OF INVENTORY AND SALES SYSTEM FOR PANDAYAN SCHOOL SUPPLIE’S STORE**

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:

Baquilar, Lovely B.

Ebona, Sheila D.

Tamparong, Meldrin

Tapitan, Reylyn B.

October 2025

**MAINTENANCE DOCUMENTATION**

**INTRODUCTION**

The Inventory and Sales System for Pandayan School Supplie’s Store is a Visual Basic 2010-based application designed to help manage inventory and sales more efficiently. Its main purpose is to replace manual tracking with a digital solution that improves accuracy, speeds up daily tasks, and supports better decision-making for store operations.

Maintenance is important to keep the system working properly over time. It helps avoid errors, ensures smooth performance, and protects the system from possible issues especially during busy seasons like the start of the school year. Without regular maintenance, the system may slow down, become outdated, or face security risks.

The scope of maintenance includes software updates, bug fixes, and security patches to make sure the system stays reliable, secure, and efficient for daily use.

**MAINTENANCE PLAN**

To ensure the long-term reliability and performance of the Inventory and Sales System for Pandayan’s School Supply Store, a proper maintenance strategy is essential. Maintenance keeps the system updated, secure, and responsive to the store’s changing needs especially during high-demand periods like the start of the school year.

**Overall Strategy**

The system will be regularly checked, updated, and improved to avoid errors, adapt to new requirements, and maintain smooth operations. Maintenance tasks will be scheduled and performed as needed to keep the system running efficiently and securely.

**Types of Maintenance Included**

* **Corrective Maintenance** – Fixes bugs, issues, and system errors that affect functionality.
* **Adaptive Maintenance** – Applies changes when there are updates in hardware, software, or business processes.
* **Perfective Maintenance** – Enhances system performance, improves user experience, and adds new features.
* **Preventive Maintenance** – Regular updates and checks to avoid future problems and system failures.

**MAINTENANCE SCHEDULE**

To ensure the system remains reliable and performs well over time, regular maintenance tasks are scheduled and assigned to specific team members. These tasks help prevent issues, fix errors, and keep the system updated and secure.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Task | Description | Frequency | Responsible Person | Status |
| Database backup | Create full backups of the database. | Weekly | Manager Name | Completed |
| Security Updates | Apply patches and updates to the system. | Monthly | Dev Team | Scheduled |
| Bug Fixes | Fix reported errors or issues. | As needed | Support Team | Ongoing |
| System Performance Check | Monitor system performance and optimize. | Quarterly | IT Team | Completed |

*Table 1: Maintenance Schedule*

**ISSUE TRACKING & BUG REPORTS**

This section contains a log of reported issues in the system, including their strictness, who reported them, and the current status. Tracking bugs helps the team respond quickly, fix errors, and improve system performance over time.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Issue ID | Description | Severity | Reported By | Date Reported | Status |
| BUG001 | Login page does not load. | High | User A | 09/28/2025 | Fixed |
| BUG002 | Payment gateway error. | Critical | User B | 10/05/2025 | In Progress |

*Table 2: Issue Tracking & Bug Reports*

**BACKUP & RECOVERY PLAN**

To protect important data and ensure business ongoing operations, the system includes a backup and recovery strategy that helps prevent permanent data loss and supports fast recovery during system failures.

**Backup Strategy**

* **Automatic Backups** – The system performs regular automatic backups of the database every week.
* **Local & Cloud Storage** – Backup files are stored both locally (on a secure drive) and in cloud storage to ensure redundancy and easy access.
* **Admin Responsibility** – The system administrator is in charge of monitoring and verifying backup completion.

**Recovery Steps**

1. **Identify the issue** – Check if the problem is caused by hardware failure, software error, or accidental deletion.
2. **Notify the IT/Admin team** – Report the issue immediately to the responsible personnel.
3. **Access backup files** – Retrieve the latest backup from local or cloud storage.
4. **Restore the database** – Use the backup file to restore system data and resume operations.
5. **Test the system** – Verify if all modules are working properly after recovery.
6. **Log the incident** – Record the issue and recovery process for future reference and improvement.

**BACKUP PROCEDURES**

To protect system data and ensure fast recovery during errors or failures, regular backups are performed and stored in multiple secure locations.

**Frequency of Backups**

* **Weekly Backups** – Full database backups are scheduled every week to keep records updated.
* **As Needed** – Additional backups may be done manually before major updates or changes.

**Storage Locations**

* **Local Server** – Backup files are saved on a secure local drive for quick access.
* **Cloud Storage** – Copies are uploaded to cloud storage for remote access and extra protection.
* **External Drive** – A portable external drive is used as a third backup option for added safety.

**RECOVERY STEPS**

In case of system failure or data loss, the following steps will guide the team in restoring the backup and resuming operations smoothly.

**Steps to Restore a Backup**

1. **Identify the issue** – Check if the failure is due to hardware, software, or accidental deletion.
2. **Notify the technical team** – Inform the system administrator or IT support immediately.
3. **Access backup files** – Locate the latest backup from local storage, cloud, or external drive.
4. **Restore the database** – Use the backup file to recover lost data and system functions.
5. **Test the system** – Make sure all modules are working properly after restoration.
6. **Log the incident** – Record the issue and recovery actions for future reference.

**Contact Information for Technical Support**

* **System Administrator:** Reylyn Tapitan
* **Email:** reylynbtapitan@gmail.com
* **Phone:** 09918597323
* **Support Hours:** Monday to Friday, 9:00 AM – 5:00 PM

**PERFORMANCE MONITORING**

To ensure the system runs smoothly and meets user expectations, key performance indicators are used to monitor system health. These metrics help identify issues early and maintain best performance.

|  |  |  |  |
| --- | --- | --- | --- |
| Metric | Description | Threshold | Monitoring Tool |
| Server Uptime | Percentage of time system is online | 99.9% | AWS CloudWatch |
| Response Time | Time taken to load pages | < 2 sec | Google Lighthouse |
| Error Rate | Percentage of failed requests | < 1% | Log Analyzer |

*Table 3: Performance Monitoring*

**SECURITY MEASURES**

To protect system data and prevent unauthorized access, the following security policies and technical safeguards are implemented.

**Security Policies & Measures**

* **Regular Updates** – The system is updated monthly to resolve system flaws and apply security fixes.
* **User Awareness** – Users are trained to follow safe login practices and avoid sharing credentials.
* **Data Protection** – Sensitive data is stored securely and only accessible to allowed users.

**Access Control Rules**

* **Role-Based Access** – Users are assigned roles (Manage, Cashier) with specific permissions.
* **Restricted Modules** – Only authorized roles can access critical modules like database settings and payment processing.
* **Session Timeouts** – Logout after inactivity to prevent unauthorized access.

**Authentication Mechanisms**

* **Username & Password** – All users must log in using unique log in details.
* **Two-Factor Authentication (2FA)** – Optional 2FA adds an extra layer of security for admin accounts.
* **Login Attempt Limits** – Accounts are temporarily locked after multiple failed login attempts.

**Encryption Methods**

* **Data Encryption** – Sensitive data (passwords, transactions) is encrypted using industry-standard algorithms.
* **Secure Connections** – All data transfers use HTTPS to protect information during transmission.
* **Encrypted Backups** – Backup files are encrypted before storage to prevent unauthorized access.

**DOCUMENTATION UPDATES**

This section records all changes made to the system documentation to reflect updates, improvements, or corrections. Keeping this log helps ensure that all team members are working with the latest and most accurate information.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Updated By** | **Section Changed** | **Description of Change** |
| 09/29/2025 | Reylyn Tapitan | Backup & Recovery Plan | Added cloud storage and recovery steps |
| 10/05/2025 | Sheila Ebona | Security Measures | Revised access control roles and added session timeout details |
| 10/13/2025 | Lovely Baquilar | System Overview | Rephrased system purpose and scope to match actual project setup. |

*Table 4: Documentation Updates*

**CONCLUSION AND RECOMMENDATION**

The team successfully completed all scheduled maintenance tasks, including weekly database backups, bug tracking and resolution, performance monitoring, and documentation revisions. These efforts helped maintain system stability, protect data, and ensure smooth operations.

For future improvements, it is recommended to implement automated alerts for system errors, add real-time monitoring dashboards, and conduct quarterly security audits. Enhancing user training on login safety and continuing to update documentation for clarity and accuracy will also improve usability and team collaboration