PET VISIT RECORD SYSTEM FOR PETLINK CALOOCAN

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:

Perez, Jocella Mae V.

October 2025

MAINTENANCE DOCUMENTATION

INTRODUCTION

The primary purpose of this documentation is to formally detail the comprehensive plan for maintaining the Pet Visit Record System (PVRS). System maintenance is not merely about fixing what is broken; it is a required, ongoing process to ensure the long-term success and dependability of the PVRS at PetLink Caloocan. The system must consistently stay reliable, perform quickly, and protect sensitive patient data over its entire operational life. Without a formal and structured maintenance plan, the system's efficiency would slowly decrease, leading to increased errors, slow operating speeds, and eventual security failures.

The PVRS is a crucial tool because it manages all daily clinic operations, including patient record-keeping and appointment scheduling. Therefore, this documentation establishes a shared, structured approach for handling all necessary updates and support activities.

The scope of this plan is comprehensive, covering all necessary activities to support the PVRS, including:

1. Correcting Errors: Fixing any mistakes or 'bugs' in the system.

2. Making Changes: Updating the system when the clinic's computers or rules change.

3. Improving Speed: Making the system run faster and easier to use.

4. Security: Protecting the system from threats and unauthorized use.

MAINTENANCE PLAN

The overall strategy for maintaining the Pet Visit Record System (PVRS) is built upon four necessary types of activities. This structured approach is essential to keep the system working correctly, adapt it to new technology, and stop problems before they can start. This plan ensures that all issues—from immediate errors that stop work to long-term improvements—are managed efficiently

Type of Maintenance	Description	Purpose
Corrective Maintenance	Fixing mistakes or errors ('bugs') that staff find and report.	To fix problems that stop the system from working correctly.
Adaptive Maintenance	Changing the system when computer environments (like a new operating system) or clinic policies change.	To keep the system working with new computer software and rules.
Perfective Maintenance	Improving the system's speed, making it easier to use, or adding minor helpful features.	To make the system run better and be more efficient for staff.
Preventive Maintenance	Regular checks and updates done to stop problems from happening later.	To keep the system healthy and prevent unexpected crashes.

MAINTENANCE SCHEDULE

This table clearly defines the Maintenance Schedule, showing exactly when specific tasks will be performed and who is responsible for the work. This schedule is a crucial part of Preventive Maintenance, as it ensures that regular, necessary checks and updates are not missed, which helps stop future problems from happening.

Task	Description	Frequency (How Often)	Responsible Person	Status
Database Backup	Making a full copy (backup) of all patient data. This is done to prevent catastrophic data loss.	Weekly	Admin Name	Ongoing
Security Updates	Putting in needed security fixes and general system updates (patches). This protects the system from new threats.	Monthly	Dev Team	Scheduled
Bug Fixes	Fixing errors or issues reported by the clinic staff	As needed	Support Team	Pending

Task	Description	Frequency (How Often)	Responsible Person	Status
	through the Issue Log (Corrective Maintenance).			
System Performance Check	Checking the system's speed and making sure it runs efficiently (Perfective Maintenance).	Quarterly (Every three months)	IT Team	Not Started

ISSUE TRACKING AND BUG REPORTS

This section details the formal process for Issue Tracking and Bug Reporting. Establishing a strict, reliable system is a fundamental requirement for Corrective Maintenance in any research or professional system. This process ensures that every problem or error found by staff is formally recorded, prioritized, and managed until it is completely solved. This is critical for maintaining system integrity and providing data for future Perfective Maintenance efforts.

All staff must report problems using a single Issue Log (a shared document or simple ticketing system) to avoid confusion and ensure central management. The logged issue acts as a verifiable record of the problem's existence, severity, and resolution.

Issue ID	Description	Severty	Reported By	Date Reported	Status
BUG001	Login page does not load	High	User A	MM/DD/YYYY	Fixed
BUG002	Cannot save a new appointment.	Critical	User B	MM/DD/YYYY	In Progress

BACKUP AND RECOVERY PLAN

This section presents the Backup and Recovery Plan, which is an essential strategy to protect the Pet Visit Record System (PVRS) from catastrophic failures, such as server hardware failure, database corruption, or malicious attacks. Since the PVRS holds all critical patient data, this plan ensures the clinic can restore operations quickly and minimize the impact of any data loss, safeguarding the continuity of care for the animals. The plan has two main components: data protection (backup) and disaster response (recovery).

Backup Procedures (Data Protection)

The backup procedure defines how frequently copies of the data are made and where they are securely stored, ensuring that a recent copy of the database is always available.

- **Frequency:** Backups of the entire database will be created Weekly. A weekly frequency provides a strong balance, as it limits any potential data loss to a maximum of seven days' worth of records, which is manageable for the clinic.

- **Storage Locations:** To follow the best practice known as the 3-2-1 Rule (though simplified for a local system), backups must be stored in two different locations:

  1. **Local Server:** A copy is kept directly on the PVRS server for the fastest possible recovery.

  2. **External Storage:** A second copy must be saved on a separate device, such as an external hard drive or a network-attached storage (NAS) device. This protects the data if the main server physically fails or is damaged.

Recovery Steps (Disaster Response)

The recovery procedure is a step-by-step guide used in an emergency to bring the PVRS back online using a recent backup file. Time is critical during recovery, so these steps are designed to be fast and clear.

Stop System Immediately - The technical lead must quickly shut down all PVRS and database services. This prevents any existing corruption from spreading or causing further damage to the remaining files.

Identify Latest Backup - Locate the most recent, verified weekly backup file from the external storage location (as per 5.1).

Restore Database - Use the local server management tools (like XAMPP's database utility) to overwrite the damaged database with the data from the identified backup file. This process reinstalls the patient records and system settings.

Restart and Verify - Start the PVRS application services and test the main functions (like searching for a pet record or creating a new appointment). If these core functions work, the system is considered operational.

Contact Support - If the restoration process fails at any point, the designated technical support team must be contacted immediately to execute a more complex, high-level restoration.

PERFORMANCE MONITORING

This section details the strategy for Performance Monitoring, which is a key part of Perfective and Preventive Maintenance. Performance monitoring is the formal process of tracking the system's speed and health to ensure it always runs efficiently for the clinic staff. By consistently measuring performance, the maintenance team can find and fix problems that cause slowdowns before they become major issues. This practice protects the system's reputation and ensures staff productivity is never harmed by slow software.

Key Performance Indicators (KPIs)

The system's health will be measured using clear metrics called Key Performance Indicators (KPIs). These metrics allow for objective evaluation of the PVRS's speed and reliability.

Metric	Description	Threshold (Goal)	Importance
Server Uptime	The total percentage of time the PVRS server is online, running, and available for staff to use.	99.9% (Must be available almost all the time)	This metric is critical as the PVRS is a local, offline system. If the server is down, clinic work stops completely.
Response Time	The measurement of how long it takes (in seconds) for the system to load a page or complete a task after a user clicks a button (e.g., retrieving a pet's record).	Less than 2 seconds	Fast response time is crucial for staff satisfaction and efficiency. Delays over 2 seconds can disrupt the workflow.

Monitoring Procedures

The Quarterly System Performance Check (as defined in the Maintenance Schedule) will specifically involve**:**

1. **Log Analysis:** Checking system logs for repeated error messages, which can show where future bugs might appear.

2. **Resource Usage Review:** Monitoring the server's Central Processing Unit (CPU) and Random Access Memory (RAM) consumption to ensure the system is not overloading the clinic's dedicated hardware.

3. **Optimization:** If any KPI falls below the target Threshold, the team will take immediate steps (Perfective Maintenance) to optimize the database queries or application code to restore performance.

SECURITY MEASURES

This section outlines the Security Measures implemented within the PVRS. As the system handles sensitive pet owner and patient data on a local server, maintaining strong security is a non-negotiable component of Preventive Maintenance. These measures protect the system from unauthorized access and potential data breaches, which is vital for maintaining the clinic's trust and data privacy.

Access Control

The system enforces strict access rules. All users must log in using unique credentials. Once logged in, their access is limited based strictly on their Job Role (e.g., a Staff user cannot view or change the higher-level financial settings reserved for an Administrator). This rule prevents accidental or intentional misuse of sensitive features.

Authentication (Password Policy)

Strong password policies are required and enforced for all user accounts. Passwords must meet minimum requirements (e.g., minimum length, use of special characters) to ensure they are difficult to guess. This is the first line of defense against unauthorized entry.

Data Protection

Technical protocols are in place to secure the database itself. Since the data is stored locally, measures are used to protect the database files from being directly accessed or changed by unauthorized people on the local network.

DOCUMENTATION UPDATES

Maintaining accurate documentation is essential for system longevity and is a core part of Adaptive Maintenance. Whenever the PVRS is modified, the supporting documents must be updated immediately to reflect those changes. This ensures that new staff, support teams, or future developers have correct and current information.

Mandatory Updates

Every time a change is implemented (whether it is a bug fix, a new small feature, or an update to the server environment), the relevant manuals must be updated. This includes the User Manual, the Troubleshooting Guide, and this Maintenance Documentation.

Version Control

All documents will use version numbers and dates to show when they were last changed. This provides a clear history of system evolution.

Goal

The primary goal is to ensure that the documentation always matches the currently running version of the PVRS, eliminating confusion and speeding up future maintenance work.

CONCLUSION AND RECOMMENDATIONS

In conclusion, the maintenance plan for the PVRS is robust, integrating four essential types of software support to guarantee system health: Corrective (fixing bugs using the Issue Log), Adaptive (changing the system to match new technology), Perfective (making it faster and easier to use), and Preventive (stopping problems through the scheduled updates). The implementation of weekly backups and strict security measures confirms the system is stable and reliable for PetLink Caloocan.

Recommendations for Future Improvements:

Based on this maintenance framework, the following recommendations are made for the future development and management of the PVRS:

1. **Automate Backups:** We strongly recommend replacing the manual Weekly Backup task with an automated tool. Automated backups are more reliable and ensure that backup copies are never missed, further securing critical patient data.

2. **Regular Refresher Training:** Refresher training should be scheduled for staff every six months. This ensures staff are using the system's features efficiently and are kept up-to-date on any minor system changes, maximizing the return on the system investment.

3. **System Technology Review:** A formal review of the system's underlying technology platform should be conducted yearly. This prevents the PVRS from becoming outdated, which is necessary for maintaining both security and high performance in the future.