In partial fulfillment of the requirements in the course

**Barangay Residents Data Management System**

**System Integration and Architecture I**

**IT 2A / Mon 5:30 - 7:30 – Thurs 5:30 – 8:30**

Submitted by:

|  |  |
| --- | --- |
| **Name** | **Student Number** |
| John Joshua T. Bandola | 23-00782 |
| Jovylene T. Siacor | 23-00781 |
| Ashley Nicole M. Badinas | 23-01518 |
| Cielo May P. Oyangorin | 23-01368 |
|  |  |

Submitted to:

**MR. JONNIFER C. MANDIGMA**

Subject Instructor

Date Submitted:

**Table of Contents**

**1 Introduction**

1.1 Purpose …………………………………………………………………………….

1.2 Project Background ……………………………………………………………….

1.3 Business Objectives ……………………………………………………………….

1.4 Project Scope ………………………………………………………………..

1.5. Project Objectives ………………………………………………

**2 Identified Risk, Assumption and Constraints**

2.1 Identified Risk ………………………………………………

2.2 Assumptions …………………………………………………..

2.3 Constraints ……………………………………………………….

**3 Proposed System Overview1**

3.1 Description of the Proposed System ……………………………………………..

3.2 System User Profile ………………………………………………………………………

3.3 Use Case Diagram ………………………………………………………………………..

3.4 Data Flow Diagram ……………………………………………………………………..

**4 Architectural Design1**

4.1 High Level components and Interfaces

4.1.1 Components …………………………………………………………………

4.2.2 Interfaces …………………………………………………………………….

4.2 Physical Arrangement of Devices in a Typical Network ……………….

4.3 User Flow Diagram ……………………………………………………………………

4.4 Use Case Diagram ……………………………………………………………………

4.5 Context Diagram ……………………………………………………………………..

**5 Functional and Non Functional Requirement1**

5.1 Functional Requirement ………………………………………………………..

5.1.1 Functional Requirement Description ………………………

5.2 Non Functional Requirements ………………………………………………

5.2.1. System Audit …………………………………………………………

5.2.2 System Control ……………………………………………………..

5.2.3 System Security ……………………………………………………………

5.2.4 Backup and Disaster Recovery …………………………………………………………

5.2.5 Usability of the Requirement …………………………………………………………..

5.2.6 System Availability …………………………………………………………….

5.2.7 System Performance ……………………………………………………………

5.2.8 Number of Users and IT Equipment ……………………………………………….

**6 Software Model and Design1**

6.1 Software Development Model ……………………………………………………………

6.2 Sequence Diagram …………………………………………………………………

6.3 ER Diagram ……………………………………………………………………..

6.4 Database Schema ……………………………………………………………

6.5. User Interface Design ………………………………………………………………………

6.5.1 Rules and Guidelines for User Interface Designing ………………

6.5.1.1 User Input Validation Methods ……………………………

6.5.1.2 Error Message, Warnings and Supportive Information …

6.5.1.3. Guideline for Interface Designing ………………………………

6.5.2 Interfaces for Each Use Case ……………………………………………………

**CHAPTER I**

**Introduction**

**1.1 Purpose:**

The purpose of the Barangay Residents Data Management System (BRDMS) is to centralize, secure, and streamline the management of all essential records within the barangay. This includes resident profiles, blotter and complaint records, clearance issuances, and other vital documents that are commonly required for legal, employment, and administrative purposes. By using BRDMS, the barangay can efficiently track individual records, verify applicant eligibility for clearances, and provide quick, accurate, and transparent services to constituents.

**1.2 Project Background**

In many barangays, resident records and clearance requests are still processed manually. This manual approach often results in delays, duplicate entries, data inconsistencies, and difficulty in verifying the authenticity of records.

When individuals apply for barangay clearance, staff must manually check physical files for any pending blotter or criminal records, which is time-consuming and prone to human error. These inefficiencies can negatively affect service quality and transparency.’

The **Barangay Residents Data Management System (BRDMS)** is designed to address these challenges by providing a centralized digital platform that maintains accurate, up-to-date resident information, automatically flags individuals with unresolved records, and streamlines clearance processing. This modernization aligns with the barangay’s goal of improving governance and citizen satisfaction.

**1.3 Business Objectives**

The BRDMS aims to:

* **Digitize and centralize records** of all barangay residents for quick access and retrieval.
* **Automate clearance verification** to minimize human error and prevent unauthorized issuance.
* **Improve operational efficiency** by reducing processing time for requests and reports.
* **Enhance transparency and accountability** in barangay recordkeeping.
* **Strengthen data security** to protect sensitive resident information from unauthorized access.

**1.4 Project Scope**

The BRDMS will cover the following functionalities:

* **Resident Profile Management** – Creation, updating, and secure storage of personal information and supporting documents.
* **Blotter and Complaint Tracking** – Recording and updating cases linked to residents.
* **Clearance Processing** – Automated verification against the database before issuing barangay clearance.
* **Document Management** – Storage of certificates, IDs, and other related files.
* **Search and Reporting Tools** – Search by name, address, or case history and generate monthly/annual reports.
* **Role-Based Access Control** – Ensuring that only authorized barangay staff can access or modify specific records.

The system will be used exclusively by barangay officials and authorized personnel. It will be hosted on the barangay’s local server or intranet to ensure secure access.

**1.5 Project Objectives**

The main objective of the Barangay Residents Data Management System (BRDMS) is to design and implement a secure, centralized, and efficient digital platform that streamlines the recording, verification, and management of barangay data. This system will replace outdated manual processes with an automated solution, ensuring faster transactions, greater accuracy, and enhanced transparency in handling resident profiles, blotter records, complaints, settlements, and clearance issuance.

Specifically, the BRDMS seeks to:

**Centralize Resident Records** – Establish a complete and well-organized digital profile for every resident, including personal information, proof of residency, and historical records, to ensure data accessibility and accuracy.

**Streamline Clearance Processing** – Facilitate faster issuance and verification of barangay clearances through automated checks for complaints, blotter entries, and flagged records.

**Ensure Data Accuracy and Consistency** – Reduce errors and redundancies by maintaining a unified database accessible only to authorized personnel.

**Promote Transparency and Accountability** – Implement a detailed audit trail of all updates, transactions, and document issuances to strengthen trust and governance.

**Enhance Search and Reporting Capabilities** – Provide advanced search and filtering tools to locate records quickly and generate accurate, timely reports for barangay officials.

**Support Data-Driven Decision-Making** – Offer reliable analytics and summaries that help barangay leaders plan community programs, monitor trends, and respond effectively to residents’ needs.

By achieving these objectives, the BRDMS will not only improve the efficiency and

reliability of barangay operations but also reinforce public trust through secure,

transparent, and well-managed information handling.

**CHAPTER II**

**Identified Risk, Assumption and Constraints**

**2.1 Identified Risk**

|  |  |  |
| --- | --- | --- |
|  | **RISK** | **MITIGATION** |
| **Data Integrity and**  **Confidentiality** | The system manages  sensitive resident  information. There is a  potential risk of data  exposure or unauthorized  access, either from external  actors or internal staff  without proper clearance.  Although residents  themselves do not directly  use the system, safeguarding  the confidentiality and  accuracy of data is essential  to ensure compliance with  the Data Privacy Act of 2012  and to maintain the trust of  the community. | Enforce role-based access,  strong authentication, and  encryption. Restrict access to  authorized staff/admins only.  Conduct regular audits,  maintain logs, and apply  barangay-level data privacy  policies. |
| **System Downtime / Service**  **Disruption** | Possible technical issues,  server crashes, or power  interruptions could  temporarily halt services  such as certificate requests  and record lookups. | Schedule regular  maintenance, prepare  backup servers and  uninterruptible power supply  (UPS), and implement a  contingency manual logging  process during outages. |
| **Data Availability and**  **Recovery** | Hardware failures, system  crashes, or accidental  deletion could result in loss  of important barangay  records. | Automate database backups  with both local and cloud  storage. Provide redundancy  and implement a data  recovery protocol to quickly  restore lost files. |
| **User Resistance to Change** | Some barangay staff may  resist transitioning from  manual paper-based  processes to the digital  system due to lack of  familiarity with technology. | Conduct capacity-building  and user training sessions.  Provide manuals/tutorials  and on-demand technical  support until users are  confident with the system. |
| **Input Errors / Inaccurate**  **Data Entry** | Incorrect or incomplete data  entry by staff could lead to  inaccurate resident records  and errors in certificate  issuance. | Enforce data validation  checks, provide verification  protocols, and assign a data  reviewer role before records  are finalized. |
| **Limited Technical**  **Infrastructure** | Barangays may have limited  computers, low processing  power, or unreliable internet  connections, affecting system  usage. | Design the system to be  lightweight and offline-  capable through local  intranet functionality.  Optimize the system to run  on existing hardware with  minimal resource  consumption. |
| **Security Threats (Viruses /**  **Malware)** | Unauthorized installation of  applications or cyber threats  may damage or compromise  the system. | Install updated antivirus  software, configure firewalls,  and apply regular system  updates and patches. |
| **Scalability Issues** | Over time, the barangay  population grows, and new  services may be required.  The system may face  performance issues if not  designed to scale. | Use a scalable database  design (normalized, modular,  expandable). Ensure the  system allows for future  integration of additional  barangay services. |

**2.2 Assumption**

|  |  |  |
| --- | --- | --- |
|  | **Assumption** | **Mitigation Strategy** |
| |  | | --- | | **Cooperation from Barangay Officials** | | Barangay staff are assumed to have basic computer skills and familiarity with common software applications. It is also assumed that officials and staff will actively participate in training and use of the system | To help barangay staff and officials, give basic computer training, easy-to-follow manuals, and video guides. Offer support and helpdesk services during the first stages. Involve officials early, explain the benefits of the system, listen to their feedback, and choose local leaders to help promote and guide others in using the system. |
| **Availability of Existing Hardware** | Each office is assumed to have at least one functioning computer meeting the minimum system requirements. | Conduct a pre-deployment hardware audit. Allocate a portion of the budget for hardware upgrades or replacements where necessary. Provide minimum specs guidance |
| **Data Availability** | Existing and accessible resident records are assumed to be available for digitization. | Plan for manual data encoding if digital records are unavailable. Train staff on record digitization. Ensure proper data collection procedures are followed |
| **Security Compliance** | Barangay offices are assumed to follow best practices in data security, access control, and password management. | Prepare a detailed cost estimate and present it to decision-makers. Identify potential funding sources (e.g., LGU grants, NGO support). Prioritize critical features if budget is limited |
| **Sufficient Budget Allocation** | There is assumed to be an adequate budget for system development, training, and minor hardware upgrades. | Coordinate early with LGU IT departments. Schedule support availability in advance. Develop contingency support plans including third-party assistance if needed. |

**2.3 Constraints**

|  |  |  |
| --- | --- | --- |
|  | **Constraints** | **Impact** |
| **Limited Scope of**  **Coverage:** | The system is limited  to barangay-level  operations and does  not connect to  municipal or national  databases. | This may restrict  data sharing across  agencies and limit  wider integration. |
| **Resource and**  **Budget**  **Limitations:** | The project must  work with limited  financial and  technical resources,  excluding advanced  features like cloud  hosting or biometric  systems. | System scalability  and long-term  expansion may be  limited. |
| **Time Constraint:** | Development and  deployment must be  completed within the  academic/project  timeline. | Only essential  features can be  prioritized, while  additional  functionalities may  be left out. |
| **Manual Data**  **Input:** | Certain records such  as criminal cases  need to be encoded  manually due to lack  of external system  integration. | May cause delays  and potential human  error in data entry. |
| **Technical Skills** | Barangay staff may  have limited  technical skills in  handling new digital  systems. | The system must  remain simple and  user-friendly, but  advanced features  may not be  maximized. |
| **Legal**  **Compliance:** | The system must  comply with existing  laws and regulations  such as the Data  Privacy Act of 2012  and LGU policies. | Failure to comply  may lead to legal  issues, penalties, or  restrictions on  system use. |

**CHAPTER III**

**Proposed System Overview1**

**3.1 Description of the Proposed System**

* The **Barangay Residents Data Management System (BRDMS)** is a web-based application designed to manage resident profiles, complaints/blotters, and clearance issuances in a centralized and secure database. The system streamlines the process of verifying an individual’s record when applying for barangay clearance by automatically checking if the person has pending blotters, complaints, or unresolved issues.
* It provides a role-based access control where barangay staff can encode and update data, barangay captains can approve clearances, and authorized agencies can perform read-only verification. Reports can also be generated to support administrative decisions and compliance requirements.

**A close-up of a computer screen

AI-generated content may be incorrect.3.2 System User Profile**

**A close-up of a document

AI-generated content may be incorrect.**

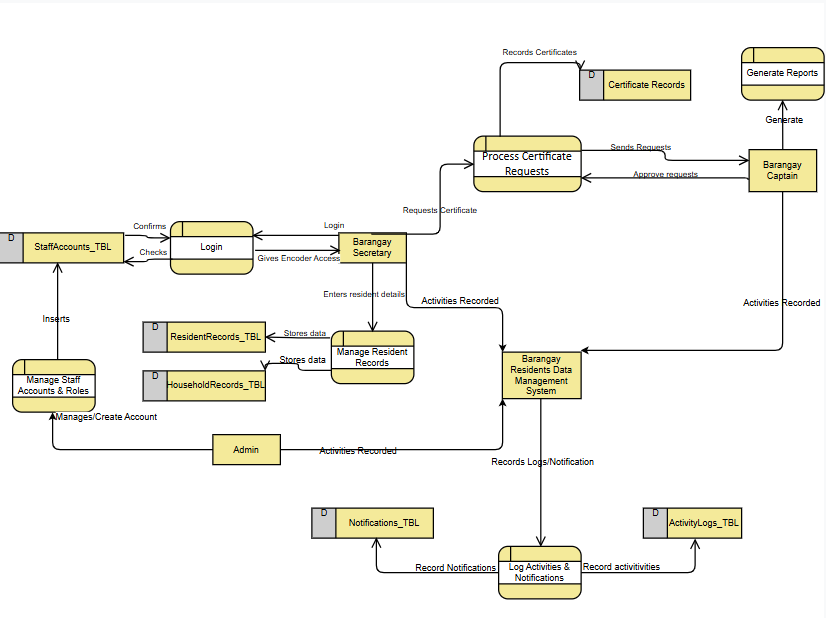
**A close-up of a document

AI-generated content may be incorrect.**

**3.3 Use Case Diagram**

**A diagram of data management system

AI-generated content may be incorrect.**

**3.4 Data Flow Diagram**

**CHAPTER IV**

**Architectural Design 1**

**4.1 High Level components and Interfaces**

**4.1.1 Components**

The Barangay Residents Data Management System (BRDMS) is composed of the following major components:

1. **User Interface (UI) Layer**

* Web-based front-end developed using **HTML, CSS, and JavaScript**.
* Provides login screens, data entry forms, search tools, and reports.

1. **Application Layer**

* Developed in **PHP**.
* Handles business logic, validation, and processing of user requests.
* Provides role-based access for **Barangay Captain, Secretary, and Staff (Viewer)**.

1. **Database Layer**

* Uses **MySQL Database**.
* Stores resident profiles, clearance records, blotter/complaints, and other official documents.
* Provides data retrieval, updates, and secure storage.

1. **Security Component**

* Authentication: Only authorized barangay officials can log in.
* Role-based authorization:
* **Barangay Captain** – Full access.
* **Barangay Secretary** – Manage records and generate reports.
* **Barangay Staff (Viewer)** – Read-only access.
* Input validation and session management to prevent unauthorized access.

**4.2.2 Interfaces**

Interfaces in the Barangay Resident Data Management System (BRDMS) for Barangay Doña Aurora, Quezon City, define how different users and system components interact with each other. Below is a breakdown of the important interfaces:

**User Interface (UI):**

● **Resident Profile Interface:** Allows barangay officers to create, update, and search resident records, including personal details and supporting documents.

● **Clearance Interface:** Provides a module for processing barangay clearance requests with automatic checks for blotter or complaint records.

● **Blotter/Complaint Interface:** Enables staff to file, update, and resolve complaints while linking them to specific resident profiles.

**Admin Interface:**

● Gives administrators full control over user accounts, system configurations, database backups, and activity monitoring to ensure security and reliability.

**Captain / Approver Interface:**  
● Allows the Barangay Captain to review clearance requests, approve or deny issuances, and access summarized reports for decision-making.

**Reporting Interface:**

● Generates automated reports such as clearance issuance summaries, blotter statistics, and resident analytics for use in barangay planning and council meetings.

**Notification Interface:**

● Sends updates and reminders to staff regarding pending clearance approvals, unresolved complaints, or flagged records.

**Authentication Interface:**

● Ensures secure logins for administrators, barangay officers, and the captain, granting access based on user roles and privileges.

**Database Interface:**  
● Connects the system to a centralized database where resident profiles, blotter records, clearance data, and system logs are securely stored and retrieved.

**4.2 Physical Arrangement of Devices in a Typical Network**

A computer diagram of a computer network

AI-generated content may be incorrect.

**4.3 User Flow Diagram**

A diagram of a company

AI-generated content may be incorrect.

**4.4 Use Case Diagram**

A diagram of data management system

AI-generated content may be incorrect.

**4.5 Context Diagram**

**A black screen with white text

AI-generated content may be incorrect.**

**CHAPTER V**

**Functional and Non-Functional Requirement1**

**5.1 Functional Requirement**

The Barangay Residents Data Management System (BRDMS) must provide the following functional requirements to support the operations of barangay staff and officials:

1. **Staff Registration and Authentication**
   * Secure login and account access for authorized barangay officials and staff with role-based permissions.
2. **Resident Record Management**
   * Recording, updating, and retrieving resident demographic and household information efficiently.
3. **Certificate and Document Processing**
   * Issuance and verification of barangay-related documents such as clearances, residency, and indigency certificates.
4. **Notifications and Alerts**
   * System-generated alerts for pending requests, follow-ups, and important system activities.
5. **Reporting and Analytics**
   * Generation of statistical, demographic, and certificate-related reports for barangay planning and decision-making.
6. **Admin Panel**
   * Administrative controls for managing staff accounts, roles, and system configurations.
7. **Security and Data Privacy**
   * Data encryption, access control, backups, and compliance with the Data Privacy Act of 2012.
8. **System Usability and Compatibility**
   * A user-friendly, responsive design accessible across desktops, laptops, and tablets, with optional offline functionality.

**5.1.1 Functional Requirement Description**

**Staff Registration and Authentication:**

●- Only authorized barangay staff and officials can register and access the system using

assigned credentials.

●- Users must log in with a verified username and password before performing any

operation.

●- The system assigns role-based access (e.g., Barangay Secretary, Treasurer, Captain,

Admin) with different levels of permission.

**Resident Record Management:**

●- Barangay staff can add and update resident profiles that contain demographic details

such as name, address, age, contact number, and household information.

●- Records are stored in a centralized database, ensuring quick retrieval and accuracy.

●- Staff may search and filter resident records using parameters like name, family ID, or

household number.

**Certificate and Document Processing:**

●- Barangay staff can generate and issue certificates such as Barangay Clearance,

Certificate of Residency, and Certificate of Indigency.

●- The system allows verification of resident information before approving and printing

documents.

**Notifications and Alerts:**

●- The system provides internal alerts for pending certificate requests and scheduled

tasks.

●- Staff members receive reminders for follow-ups, renewals, and record updates.

●- Critical system notifications (e.g., backup reminders, data errors) are sent to admin

accounts.

**Reporting and Analytics:**

●- Barangay staff can generate statistical reports based on demographics, household

data, and issued certificates.

●- Reports can be customized (daily, weekly, monthly, or yearly) to support barangay

planning and decision-making.

●- Data can be exported in PDF or Excel format for documentation and presentations.

**Admin Panel:**

●- The admin has full control to manage staff accounts, reset passwords, and assign

access roles.

●- Admins may configure barangay-specific document templates, service settings, and

system preferences.

●- The system logs all staff activities for accountability and auditing purposes.

**Security and Data Privacy:**

●- The system ensures compliance with the Data Privacy Act of 2012 by encrypting

sensitive resident information.

●- Access levels prevent unauthorized users from viewing or editing confidential data.

●- Automatic system backups are performed regularly to protect against data loss.

**System Usability and Compatibility:**

●- The system is designed to be responsive and can be accessed via desktop, laptop, and

tablets used by barangay staff.

●- A simple and user-friendly interface ensures that staff with limited technical

background can operate the system efficiently.

●- Offline mode may be supported to allow data entry without internet, with

synchronization once the connection is restored.

**5.2 Non Functional Requirements**

**5.2.1. System Audit**

**5.2.2 System Control**

System control in the Barangay Residents Database Management System (BRDMS) is essential for safeguarding sensitive data, ensuring accurate operations, and maintaining trust in barangay services. Since the system manages critical information such as resident profiles, complaints, blotters, and clearance records, strong control measures must be in place. Here are the key areas of system control that should be addressed:

**Access Control**

* The system implements **Role-Based Access Control (RBAC)**, assigning permissions according to responsibilities such as Encoder, Barangay Secretary, Barangay Captain, or Viewer.
* **User authentication** is enforced through unique login credentials, with optional **multi-factor authentication (MFA)** for administrative users.
* Access to confidential data (e.g., blotter records) is restricted strictly to authorized staff.

**Data Protection and Integrity**

* All records are encrypted **in transit (HTTPS)** and **at rest** in the database.
* Data validation rules ensure that entries such as resident details, complaints, or clearance requests are complete and accurate before saving.
* Sensitive fields (e.g., addresses, ID numbers) can be masked for non-administrative users to minimize data exposure.

**Audit and Monitoring**

* A detailed **audit trail** records user activities such as logins, record creation, updates, approvals, or deletions.
* Each log includes user ID, timestamp, and specific actions for accountability and compliance with the **Data Privacy Act of 2012**.
* Audit logs are reviewed regularly to detect anomalies or suspicious activity.

**Backup and Recovery**

* The system performs **scheduled backups** stored both locally and in secure cloud storage.
* **Disaster recovery protocols** are established to restore data quickly in the event of system crashes, accidental deletions, or hardware failures.

**System Maintenance and Change Control**

* **Patch management** ensures that BRDMS software and dependencies are updated regularly against known vulnerabilities.
* A **formal change management process** requires testing and approval of system updates or configurations before deployment to avoid service interruptions.

**Incident Response and Security Measures**

* An **incident response plan** outlines procedures for reporting, investigating, and resolving security issues.
* **Firewalls, anti-virus software, and monitoring tools** are deployed to safeguard against cyber threats and malware.
* Barangay staff undergo **security awareness training** to reduce risks caused by human error or social engineering.

**Physical and Organizational Controls**

* Servers and computers used for BRDMS are kept in **secured areas with restricted physical access**.
* User accounts are **promptly updated or revoked** when staff roles change or employment ends.

Standard operating procedures (SOPs) and barangay-level IT policies ensure **consistent compliance** and operational integrity.

**5.2.3 System Security**

System security in the Barangay Resident Data Management System (BRDMS) is essential to protecting sensitive resident information, ensuring data integrity, and maintaining public trust. Since the system handles personal and confidential records, implementing strong security measures is necessary to safeguard against unauthorized access and data breaches. The following areas of system security must be addressed:

**Authentication and Access Control:**

●- Implement strong authentication mechanisms such as unique usernames and secure

passwords for barangay staff.

●- Use Role-Based Access Control (RBAC) to ensure that only authorized staff members, such

as the barangay secretary, treasurer, or captain, can access specific system functions.

●- Apply the principle of least privilege so that staff can only perform tasks relevant to their assigned role.

**Data Encryption:**

●- Encrypt resident records and sensitive information both in transit and at rest to protect

against unauthorized access.

●- Utilize strong encryption algorithms and secure key management practices for data storage and backup files.

**Secure Communication:**

●- Use secure communication protocols such as HTTPS to encrypt data exchanges between

staff devices and the system server.

●- Apply Transport Layer Security (TLS) to ensure the confidentiality and integrity of

transmitted information.

**Vulnerability Management:**

●- Regularly scan the system for potential vulnerabilities through automated tools and

manual reviews.

●- Apply timely patches and system updates to address known security risks.

●- Conduct periodic security audits and penetration testing to identify and fix security

weaknesses.

**Secure Coding Practices:**

●- Follow secure coding standards to prevent vulnerabilities such as SQL injection, cross-site scripting (XSS), and weak authentication.

●- Use trusted development frameworks and libraries while reviewing code for potential flaws.

**Incident Response Planning:**

●- Establish an incident response plan outlining how to detect, report, and address

potential security breaches.

●- Form a barangay-level incident response team with defined responsibilities to

handle security incidents effectively.

**Data Protection and Privacy:**

●- Enforce data privacy measures including encryption, restricted access, and

anonymization where applicable.

●- Ensure compliance with the Data Privacy Act of 2012 (Philippines) to protect

resident data from misuse or unauthorized sharing.

**Employee Training and Awareness:**

●- Provide barangay staff with regular training on cybersecurity best practices and

system security policies.

●- Encourage a culture of vigilance, ensuring staff promptly report suspicious

activities or potential threats.

**Physical Security:**

●- Secure the physical server, computers, and backup storage devices within the

barangay hall or designated facility.

●- Implement access controls, surveillance cameras, and monitoring systems to

prevent unauthorized physical access to IT assets.

**5.2.4 Backup and Disaster Recovery**

A robust **Backup and Disaster Recovery (BDR) strategy** is essential for ensuring the continuity and reliability of the Barangay Residents Data Management System (BRDMS). Since the system stores sensitive and vital records such as resident profiles, clearance issuances, and blotter/complaint data, measures must be in place to protect against data loss, corruption, or system downtime caused by hardware failures, natural disasters, cyberattacks, or human errors.

**Backup Strategy**

1. **Database Backups**
   * Automated daily backups of the MySQL database will be scheduled.
   * Full backups will be performed weekly, while incremental backups will be conducted daily to save storage space.
   * Backup files will be encrypted and stored securely to prevent unauthorized access.
2. **File and Document Backups**
   * Supporting documents uploaded in the system (e.g., clearance attachments, scanned barangay forms) will be included in the backup routine.
   * Versioning will be implemented to track changes and restore previous file states if necessary.
3. **Storage Locations**
   * **Primary Backup**: Stored on a secure local server within the barangay office.
   * **Secondary Backup (Off-site/Cloud-based)**: A copy will be stored in a secure cloud storage service or an external hard drive located in a different physical location to safeguard against fire, flood, or theft.

**Disaster Recovery Plan**

1. **Recovery Objectives**
   * **Recovery Time Objective (RTO):** The system should be fully operational within **24 hours** of a major disruption.
   * **Recovery Point Objective (RPO):** No more than **24 hours of data** should be lost in the event of a failure.
2. **Disaster Recovery Procedures**
   * In case of **hardware failure**, the system will be restored from the latest backup using replacement hardware.
   * In the event of a **cyberattack (e.g., ransomware or hacking)**, compromised systems will be isolated, cleaned, and restored from unaffected backup files.
   * In case of **natural disasters (e.g., fire, flood, earthquake)**, the system will be restored from off-site or cloud backups using temporary infrastructure until the barangay office systems are restored.
3. **Testing and Validation**
   * Regular **backup verification** will be conducted to ensure the integrity and reliability of backup files.
   * Periodic **disaster recovery drills** will be performed to assess staff readiness and measure recovery efficiency.
4. **Roles and Responsibilities**
   * **Barangay Secretary:** Oversees the backup schedule and ensures compliance.
   * **Barangay Captain:** Authorizes recovery procedures in case of disaster.
   * **Barangay Staff (Viewer Role):** Reports system issues but does not handle recovery tasks.

**5.2.5 Usability of the Requirement**

The usability of the Barangay Residents Data Management System (BRDMS) ensures that all users, particularly the **Barangay Captain, Secretary, and Staff**, can interact with the system efficiently and effectively. Since the system is intended for daily administrative tasks, usability requirements focus on simplicity, accessibility, and ease of navigation.

The interface is designed to be **user-friendly**, with intuitive menus, clear labels, and minimal technical complexity. Forms for adding, updating, and searching records are structured to follow a logical workflow, reducing the learning curve even for users with limited technical knowledge. Consistency in design, such as standardized buttons and color coding, improves the overall user experience.

Accessibility is also considered, ensuring that the system can run on standard computers available in the barangay office without requiring specialized hardware. Furthermore, error messages are descriptive and guide the users toward resolving issues instead of displaying vague technical details.

The system ensures that the **captain and secretary have secure access to critical features**, while staff (viewers) are limited to data retrieval and viewing, preventing misuse of sensitive information. This role-based access improves usability by minimizing confusion over which tasks each user is allowed to perform.

Overall, the usability of the BRDMS is aligned with the principle that the system should **support the work of barangay officials and staff, not complicate it.** The system design prioritizes efficiency, accuracy, and a smooth user experience, enabling the barangay office to manage records and transactions with greater confidence and reliability.

**5.2.6 System Availability**

**5.2.7 System Performance**

The Barangay Resident Data Management System's (BRDMS) performance is crucial to

ensure smooth operations, fast data retrieval, and efficient handling of resident records. To

evaluate its effectiveness, the system’s performance is monitored using several key

performance factors. The following are the main aspects of system performance:

**Response Time:**

● The system monitors the average response time for user actions such as searching

resident records, updating information, and generating reports. The target response time is set to less than 3 seconds to ensure efficiency and user satisfaction.

**Scalability:**

● The system is designed to handle the growing number of resident records and barangay staff users without affecting performance. Scalability tests are conducted regularly to verify that the system can meet increasing data and user demands.

**Concurrency:**

● The system’s ability to manage multiple barangay staff accessing and updating records at the same time is continuously checked. It is designed to support concurrent sessions during peak usage while maintaining speed and responsiveness.

**Reliability:**

● System reliability is prioritized to ensure continuous access to resident records and

minimize downtime. The system aims for a target uptime of at least 99.9% to guarantee that barangay operations are not disrupted.

**Data Integrity:**

● Ensuring the accuracy and consistency of resident data is a top priority. The system uses validation mechanisms, regular data backups, and secure storage methods to maintain data integrity and prevent loss or corruption.

**Optimized Database Performance:**

● Database operations are optimized to ensure efficient storage and retrieval of resident

records. Techniques such as indexing, query optimization, and caching are implemented to maintain fast performance even as the database grows.

**User Experience:**

● The system is built to provide barangay staff with a smooth and intuitive user

experience. Clear navigation, responsive interfaces, and proper error handling are

implemented to minimize mistakes and improve productivity.

**5.2.8 Number of Users and IT Equipment**

**Number of Users**

The system will serve multiple categories of users with different roles and responsibilities:

1. **Barangay Captain**
   * Monitors reports, verifies records, and approves critical transactions.
2. **Barangay Secretary**
   * Manages resident profiles, prepares barangay certifications, and handles documentation.
3. **Barangay Encoders/Clerks**
   * Handles data entry for resident profiles, clearances, blotters, and complaints.
4. **System/IT Administrator**
   * Manages system operations, user access, database backups, and security enforcement.

**IT Equipment**

To support the BRDMS efficiently, the following IT equipments are required:

**1. Servers**

* **Application Server:** Runs the BRDMS web application and handles transactions.
* **Database Server:** Stores resident records, reports, and other system data.
* **Backup Server (Optional):** Maintains periodic backups for disaster recovery.

**2. Networking Equipment**

* **Router:** Connects the barangay network to the internet.
* **Switches (Managed):** Connects multiple devices and ensures stable communication.
* **Firewall:** Provides network security and blocks unauthorized access.
* **Wireless Access Points (WAP):** Ensures Wi-Fi connectivity across the barangay office.
* **Cabling:** Structured Ethernet cables (Cat6/Cat6a) for wired connections.

**3. Workstations**

**For Staff & Officials:**

* Desktop computers/laptops used by secretary, treasurer, and clerks.
* **Monitors:** At least 22-inch LED monitors for clarity in record handling.

**4. Printing and Scanning Devices**

* **Printers:** Laser or inkjet printers for clearances, reports, and certifications.
* **Scanners:** For digitizing resident IDs, complaint forms, and supporting documents.
* **Multi-Function Devices (MFPs):** Combination of printing, scanning, and photocopying.

**6. Security Equipment**

* **CCTV Cameras:** Monitors the physical environment where IT equipment is stored.
* **Biometric/Access Control Systems:** Ensures only authorized staff can access server rooms or sensitive equipment.
* **Antivirus and Endpoint Security Software:** Protects computers and servers from malware and data breaches.

**7. Backup and Disaster Recovery Systems**

* **External Hard Drives (Portable Storage):** For local backup copies.
* **Network Attached Storage (NAS):** Centralized storage solution with automated backups.
* **Cloud Backup Services:** Redundant off-site backups for disaster recovery.
* **Generator/Power Backup (Optional):** Ensures continuous system operations during extended power interruptions.

**8. Miscellaneous IT Equipment**

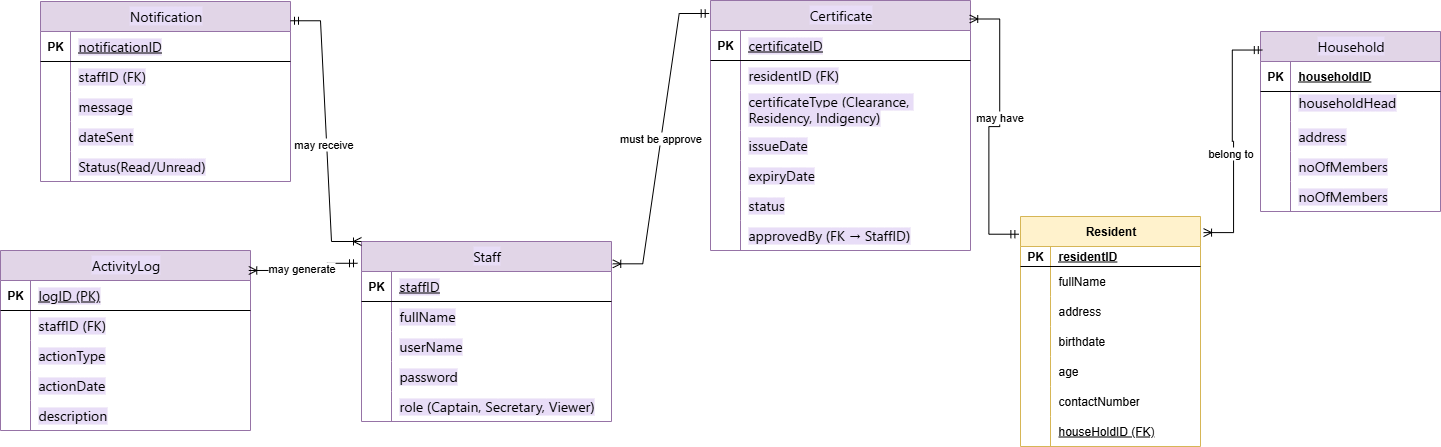
* **Keyboards and Mice:** Standard peripherals for workstations.
* **External Storage Media (USBs, DVDs):** For quick file transfer and archiving.

**Software Model and Design1**

**6.1 Software Development Model**

**6.2 Sequence Diagram**

**6.3 ER Diagram**

****

**6.4 Database Schema**

**6.5. User Interface Design**

**6.5.1 Rules and Guidelines for User Interface Designing**

**6.5.1.1 User Input Validation Methods**

**6.5.1.2 Error Message, Warnings and Supportive Information**

**6.5.1.3. Guideline for Interface Designing**

**6.5.2 Interfaces for Each Use Case**