C:\Users\Payodhi Mishra\AppData\Local\Microsoft\Windows\INetCache\Content.Word\Logo.png

# Business Requirement Document

**BRD Name**: **Field Level Encryption of Nominee Details**

## V 1.0

## BRD No: 1

# BRD History:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Prepared BY | Reviewed By | Version | Date | Tech Owner | Business Owner |
| Vijayakumar | Payodhi | V1.0 | 03/01/2024 | Shivashankar | Chandramohan |

# Change History:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev No. | Date of rev | Page No | Summary of changes | Prepared by | Status |
| V1.0 | 03/01/2024 | 3 | Field Level Encryption of Nominee Details | Vijayakumar | Completed |
|  |  |  |  |  |  |

Contents

[Business Requirement Document 1](#_Toc525137815)

[1](#_Toc525137816)

[V 1.0 1](#_Toc525137817)

[BRD No: 1](#_Toc525137818)

[BRD History: 1](#_Toc525137819)

[Change History: 1](#_Toc525137820)

1.Introduction…………………………………………………………………………………………………………………………………………………………… 3

2.Objective……………………………………………………………………………………………………………………………………………………………….. 3

3.Scope…………………………………………………………………………………………………………………………………………………………………….. 3

4.Business Requirements…………………………………………………………………………………………………………………………………………… 3

4.1 Functional Requirements………………………………………………………………………………………………………………………………… 3

4.2 Nonfunctional Requirements………………………………………………………………………………………………………………………….. 3

5.Encryption Details………………………………………………………………………………………………………………………………………………….. 4

5.1 Fields to be Encrypted…………………………………………………………………………………………………………………………………….. 4

5.2 Encryption Standards………………………………………………………………………………………………………………………………………. 4

6.Data Flow………………………………………………………………………………………………………………………………………………………………. 4

7.Assumptions and Constraints…………………………………………………………………………………………………………………………………. 4

8.Impact Analysis………………………………………………………………………………………………………………………………………………………. 4

# 1. Introduction

This document outlines the business requirements for implementing fieldlevel encryption for nominee details. The purpose is to ensure that sensitive information is protected and accessible only by authorized entities.

# 2. Objective

The objective of this project is to enhance the security of nominee details by encrypting specific fields. This will protect the data from unauthorized access and potential breaches.

# 3. Scope

The scope of this project includes:

* Identifying the nominee details that need encryption.
* Implementing encryption and decryption mechanisms.
* Ensuring compliance with industry standards and regulations.
* Testing and validating the encryption implementation.

# 4. Business Requirements

**4.1** **Functional Requirements:**

Encrypt Nominee Details: The system should encrypt the following nominee details:

* Nominee Name
* ngender
* ndob
* nage
* nrelationship
* nhouseno
* nstreatno
* nlandmark
* nlocation

2.Decrypt Nominee Details: Authorized users should be able to decrypt and view the nominee details.

3.Access Control: Ensure only authorized users have access to encryption and decryption functionalities.

4.Data Integrity: Ensure that data integrity is maintained during the encryption and decryption processes.

**4.2 Nonfunctional Requirements**

1.Performance: The encryption and decryption processes should not significantly impact the system's performance.

2.Scalability: The solution should be scalable to accommodate an increasing number of nominee records.

3.Compliance: The solution should comply with relevant data protection regulations and standards.

**5. Encryption Details**

**5.1 Fields to be Encrypted**

* NomineeName
* ngender
* ndob
* nage
* nrelationship
* nhouseno
* nstreatno
* nlandmark
* nlocation

**5.2 Encryption Standards**

* Algorithm: Advanced Encryption Standard (AES)
* Key Size: 256 bits
* Mode of Operation: Cipher Block Chaining (CBC) or Galois/Counter Mode (GCM)
* Key Management: Use a secure key management system (e.g., AWS KMS, Azure Key Vault)

**6. Data Flow**

* Data Entry: Nominee details are entered into the system.
* Encryption: Upon submission, the specified fields are encrypted.
* Storage: Encrypted data is stored in the database.

Decryption: When required, authorized users can decrypt and view the data.

**7.** **Assumptions**

All encryption keys will be securely managed and rotated regularly.

Users accessing encrypted data will have the necessary permissions.

The system will have sufficient computational resources to handle encryption and decryption tasks.

**8. Impact Analysis**

Database Schema Changes: Adjustments to store encrypted data.

Application Logic: Modifications to include encryption and decryption processes.

User Training: Training for authorized users on how to handle encrypted data.

Regularly audit access to encrypted data and encryption keys.