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

# Business Requirement Document

**BRD Name**: **Mobile OTP-Based Sourcing**

## V 1.1

## BRD No: 2

# BRD History:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Prepared BY | Reviewed By | Version# | Date | Tech Owner | Business Owner |
| Vijayakumar | Payodhi | V1.1 | 28/11/2024 | Shivashankar | Chandramohan |

# Change History:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Rev No. | Date of rev | Page No | Summary of changes | Prepared by | Status |
| V1.1 | 28/11/2024 | 3 | Mobile OTP-Based Sourcing | Vijayakumar | Completed |
|  |  |  |  |  |  |

Contents

[Business Requirement Document 1](#_Toc525137815)

[1](#_Toc525137816)

[V 1.1 1](#_Toc525137817)

[BRD No: 1](#_Toc525137818)

[BRD History:. 1](#_Toc525137819)

[Change History: 1](#_Toc525137820)

[1 Introduction: 3](#_Toc525137821)

1.1 Purpose:………………………………………………………………………………………………………………………………………………………….. 3

1.2 Scope:…………………………………………………………………………………………………………………………………………………………….. 3

1.3 Stakeholders:…………………………………………………………………………………………………………………………………………………. 3

2 Business Requirements……………………………………………………………………………………………………………………………………….. 3

2.1 Mobile OTP-Based Sourcing Implementation:……………………………………………………………………………………........... 3

2.1.1 Requirement Description…………………………………………………………………………………………………………………………… 3

2.1.2 Functional Requirements…………………………………...………………………………………………………………………………………. 3

2.1.3 Non-Functional Requirements…………………………………………………………………………………………………………………… 4

3 Impact Analysis……………………………………………………………………………………………………………………………………………… 4

4 **Assumptions & Dependencies** …………………………………………………………………………………………………………………………… 4

5. Acceptance Criteria ……………………………………………………………………………………………………………………………………………. 4

# 1 Introduction:

**1.1** **Purpose**

This document outlines the business requirements for implementing Mobile OTP-based sourcing, ensuring secure and efficient verification of users during the sourcing process.

**1.2 Scope**

The implementation will enable user verification via OTP (One-Time Password) sent to their registered mobile number, reducing fraud and improving authentication efficiency.

**1.3 Stakeholders**

* Business Team
* IT Development Team
* Quality Assurance Team
* Product Management
* Operations Team

# 2 Business Requirements:

### 2.1 Mobile OTP-Based Sourcing Implementation

**2.1.1 Requirement Description**

* Users will receive an OTP on their registered mobile number during the sourcing process.
* The OTP will serve as an authentication step before proceeding with further data entry.
* OTPs will be time-sensitive and expire after a predefined duration.

**2.1.2 Functional Requirements**

* **OTP Generation**: System should generate a unique OTP upon user registration initiation.
* **OTP Delivery**: OTP should be sent via SMS to the registered mobile number.
* **OTP Validation**: Users must enter the correct OTP within the validity period to proceed.
* **Resend Option**: Allow users to request a new OTP after a short waiting period.
* **Failed Attempts Handling**: Lock user account temporarily after multiple failed attempts.

**2.1.3 Non-Functional Requirements**

* **Security**: OTP should be encrypted and not stored after validation.
* **Performance**: OTP delivery should be near-instant, with a success rate above 95%.
* **Scalability**: The system should handle high volumes of OTP requests concurrently.

### 3 Assumptions:

* **System Impact:** New API integrations for OTP generation and validation.
* **User Impact:** Users must provide a valid mobile number for authentication.
* **Reporting Impact:** System logs must capture OTP generation, validation, and failures.
* **Compliance Impact:** Ensure adherence to data privacy regulations.

## ****4. Assumptions & Dependencies****

* Integration with third-party SMS gateway providers.
* Mobile number database should be up-to-date.
* Adequate UAT before deployment.

**5. Acceptance Criteria**

* OTP is successfully generated and delivered to the user’s mobile.
* Users can authenticate using OTP within the specified time frame.
* The system prevents unauthorized access after multiple failed attempts.