|  |  |
| --- | --- |
| **RFC Number** |  |

*(Allotted by EPMO)*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Part A) Change Details – To be filled by Change Initiator *(Fill in with appropriate information)*** | | | | | | | | |
| **Request Title** |  | | | | | | | |
| **Requestor Name** |  | | | | | | | |
| **Request Date** (dd/mm/yyyy) |  | | | **Related RFC Number** | | |  | |
| **NIR #** |  | | | **Project Reference** | | |  | |
| **List Software / Module(s) / Report(s) to change** *– use additional sheet(s) if required* |  | | | | | | | |
| **Brief Description** *(should give high level picture of change. If a report then mention fields, search parameters )- use additional sheet(s) if required* |  | | | | | | | |
| **Reason for Change** *(justification for change i.e. due to process improvement, customer experience, regulatory, audit/compliance* |  | | | | | | | |
| **Priority** | High Medium Low | | | | | | | |
| **Date Change is Required By** |  | | | | | | | |
| **Attachments** | Yes  No | | | | | | | |
| **Change Initiator (Name, Signature & Date)** |  | | | **Business Head (Name, Signature & Date)** | |  | | |
| **Part B) Change Analysis – To be filled by IT *(Fill in with appropriate information)*** | | | | | | | | |
| **Change Impact** *(should give high level picture of change impact mentioning list of screens/reports/database structure/APIs) – use additional sheet(s) if required* |  | | | | | | | |
| **Efforts** | Mandays |  | Vendor/Inhouse?) | |  | Cost (PKR) *(if vendor involved)* | |  |
| **IT Analyst (Name, Signature & Date)** |  | | | **IT Manager (Name, Signature & Date)** | |  | | |

|  |  |
| --- | --- |
| **RFC Number** |  |

*(To be allotted by IT)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Part C) IT Quality Assurance** | | **Part D) User Acceptance** | |
| **Test Result** | Pass  Fail | Pass  Fail | |
| **QA Manager (Name, Signature & Date)** |  | **UAT Lead (Name, Signature & Date)** |  |
| **Part D) Implementation** | | | |
| **Status** | Successful  Rollback  Rollback reason: *mention reason for rollback the deployment due to any reason like technical or business decision* | | |
| **Date & Time** | *Actual date and time of deployment* | | |

|  |  |
| --- | --- |
| **RFC Number** |  |

|  |  |
| --- | --- |
| **Part A) Change Details – Additional Details** | |
| **List Software / Module(s) / Report(s) to change** | RMS Android |
| **Brief Description** *(should give high level picture of change. If a report then mention fields, search parameters )* | 1. **User Sign Up**   **Requirements:**  **Screen 1**   * User will be asked to enter following fields:   1. Employee Code   2. Password with complexity      + Minimum 6 characters and Maximum 8 characters      + Combination of Upper and lower case, special character, digits * Continue button for moving to next screen and One time password (OTP) will be generated   **Screen 2**   * User will be asked to enter One time password (OTP) * OTP will be sent on his mobile number defined against courier code which must be centrally managed somewhere in Courier profile repository * Once OTP is verified then   1. SMS will be sent on User mobile that “You have successfully registered for RMS Mobile Application”   2. User will be allowed to proceed to Main menu screen * If OTP is not verified then user will be asked for retry upto 3 times and then his ID should be locked for Sign Up * There should be OTP regenerate option enabled if OTP invalid retry count is less than ‘3’ * Only twice user can be allowed for Regenerate OTP option * Once ID is locked then he/she can sign up only through Admin function  1. **Forgot Password**   **Requirements**  **Screen 1**   * User will be asked to enter Employee Code * Continue button for moving to next screen and One time password (OTP) will be generated   **Screen 2**   * User will be asked to enter One time password (OTP) * OTP will be sent on his mobile number defined against courier code which must be centrally managed somewhere in Courier profile repository * Once OTP is verified then   1. SMS will be sent on User mobile that “You have successfully Reset your password”   2. User will be asked to Login to application * If OTP is not verified then user will be asked for retry upto 3 times and then his ID should be de-activated * There should be OTP regenerate option enabled if OTP invalid retry count is less than ‘3’ * Only twice user can be allowed for Regenerate OTP option * Once ID is locked then he/she can Admin to Reset password and activate ID |
| **Reason for Change** *(justification for change i.e. due to process improvement, customer experience, regulatory, audit/compliance* |  |

|  |  |
| --- | --- |
| **RFC Number** |  |

*(To be allotted by IT)*

|  |  |
| --- | --- |
| **Part B) Change Analysis – Additional Details** | |
| **Change Impact** *(should give high level picture of change impact mentioning list of screens/reports/database structure/APIs)* |  |