**1. Login Service**

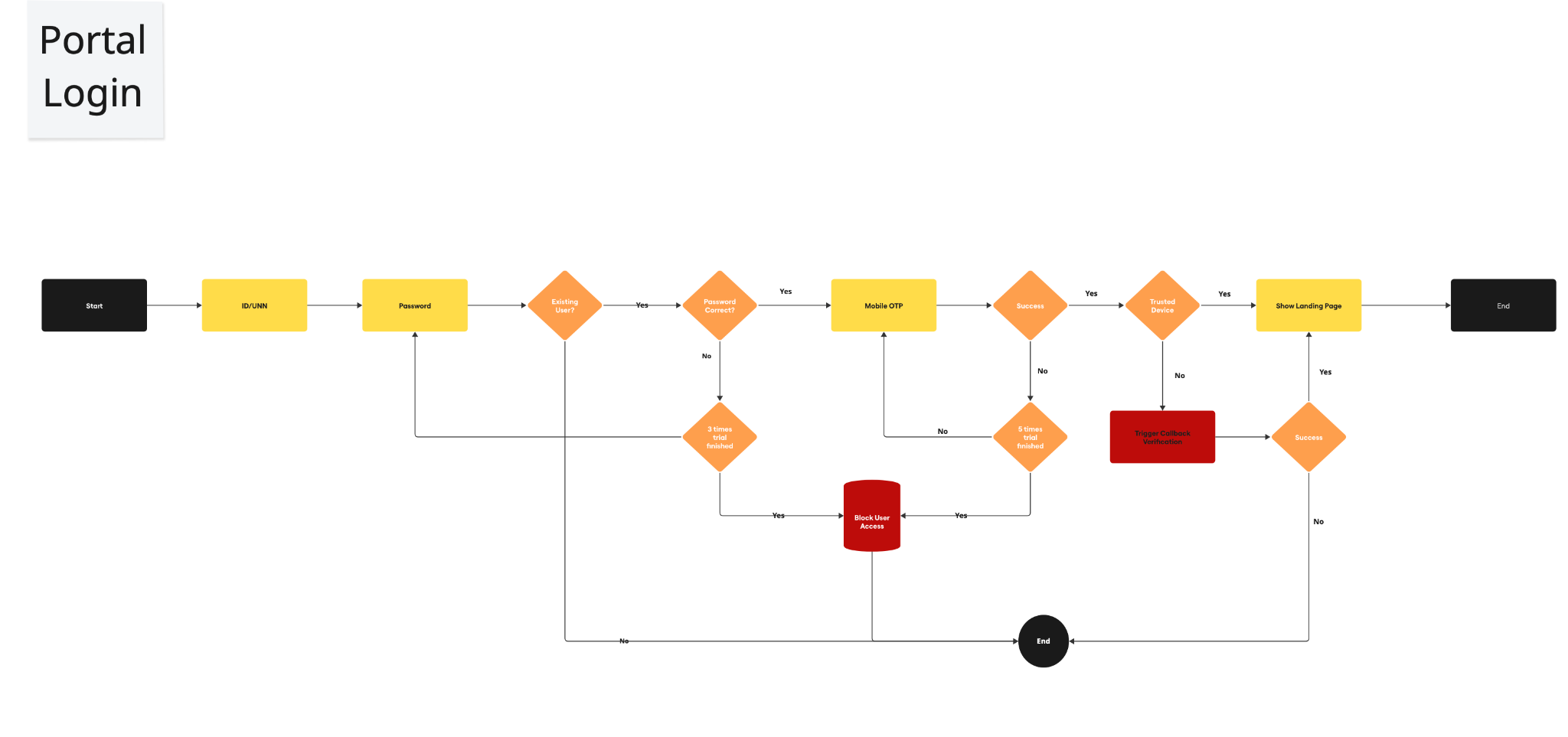
* **For “Portal”**
* **Service Description:**
* Login is the process that allows a registered user to securely access their e-wallet account using their verified credentials.
* The primary objective is to authenticate the user’s identity by validating their login information and applying security measures, such as password checks and OTP verification, to ensure safe and authorized access to the system.
* This process includes verifying:
* ID/UNN number
* Verify ID/UNN
* Password
* Verify password
* OTP validation
* Trusted device
* Verify trusted device
* **General User Story:**

"As a registered user, I would like to **log in** to my wallet account through the **portal** using secure credentials, so that I can access and manage my financial services securely."

* **Detailed** **log in Flow:**

|  |  |
| --- | --- |
| Step #1 | **ID/UNN number and Password**   * The user enters their ID/UNN number, then their password. |
| Step #2 | **Check the user in the system**   * The system checks this user:  1. If the user **exists** in the system, they move to the next step, "Password Verification." 2. If the user **doesn't exist** in the system, the process stops. |
| Step #3 | **Check the user password in the system**   * In this step, the entered password is verified.  1. If the password is **correct**, the user will proceed to the next step, which is “Mobile OTP.” 2. If the password is incorrect, the user is allowed to repeat the process (3 times).  * If the password is entered **correctly**, the user will proceed to the next step, which is **"Mobile OTP."** * If all attempts are completed **without entering the password correctly**, the process will stop and the user will be blocked. “**Block User Access**”. * The account is unblocked via forget password/reregistration. |
| Step #4 | **Mobile OTP**   * A 4-digit code will be sent to the user's mobile phone number. * Example:  |  |  | | --- | --- | | In English | In Arabic | | “Please use OTP: 1111  For: Login" | "نأمل إستخدام رمز التفعيل: ١١١١  من أجل: تسجيل الدخول" |  1. If the code is **confirmed** by the user, they will proceed to the next step, **"Trusted Device."** 2. If the code is **not confirmed**, they will only be allowed to repeat the process (5 times.)  * If **all attempts are completed without the code being entered correctly**, the user will be **blocked.** “**Block User Access**” and the process will stop. * If the user **successfully** enters the code correctly, they will proceed to the next step, **"Trusted Device."** |
| Step #5 | **Trusted Device**   * The device will be checked to see if it is **trusted or not.**  1. If the **device is trusted**, they will proceed to the next step "**Landing Page."** 2. If the device is **not trusted**, the system will take a **callback** action for the user. "**Trigger Callback Verification**"   \*\*\*\* The voice message contains,  "Dear customer, We have received a login request from a new device. If you are the one initiating this request, press 1, or press 2 for cancellation."  Arabic also:  “عزيزي العميل، لقد تلقينا طلب تسجيل دخول من جهاز جديد. إذا كنتَ أنت من بدأ هذا الطلب، فاضغط على 1، أو اضغط 2 للإلغاء”   * If the callback is **successful** and the user confirms, they will be redirected to the **"Landing Page."** * If the callback **fails**, the process stops. * The voice message text can be changed. |

* **Log in Process-Flow:**



* Note: You can also access the file via the following link:

[Portal\_Loging\_V1.pdf](https://disholding.sharepoint.com/:b:/s/Holding/EQBo7V1aBe9AutQyR5R54ngBMBeqVxtfMzgM60wn40l9tA?e=KZweSi)

**2. Login Service**

* **For “Mobile”**
* **Service Description:**
* Login is the process that allows a registered user to securely access their e-wallet account using their verified credentials.
* The primary objective is to verify the user's identity by verifying login information and applying security measures, such as password verification, one-time password (OTP) verification, passcode verification, and device trust, to ensure secure and authorized access to the system.
* This process includes verifying:
* Verifying whether the device is **linked or not**
* Verifying **biometric** login
* Verifying **passcode** login
* Verifying **password** login
* **General User Story:**

"As a registered user, I would like to log in to my wallet account **through the mobile application** using secure credentials so that I can access and manage my financial services securely."

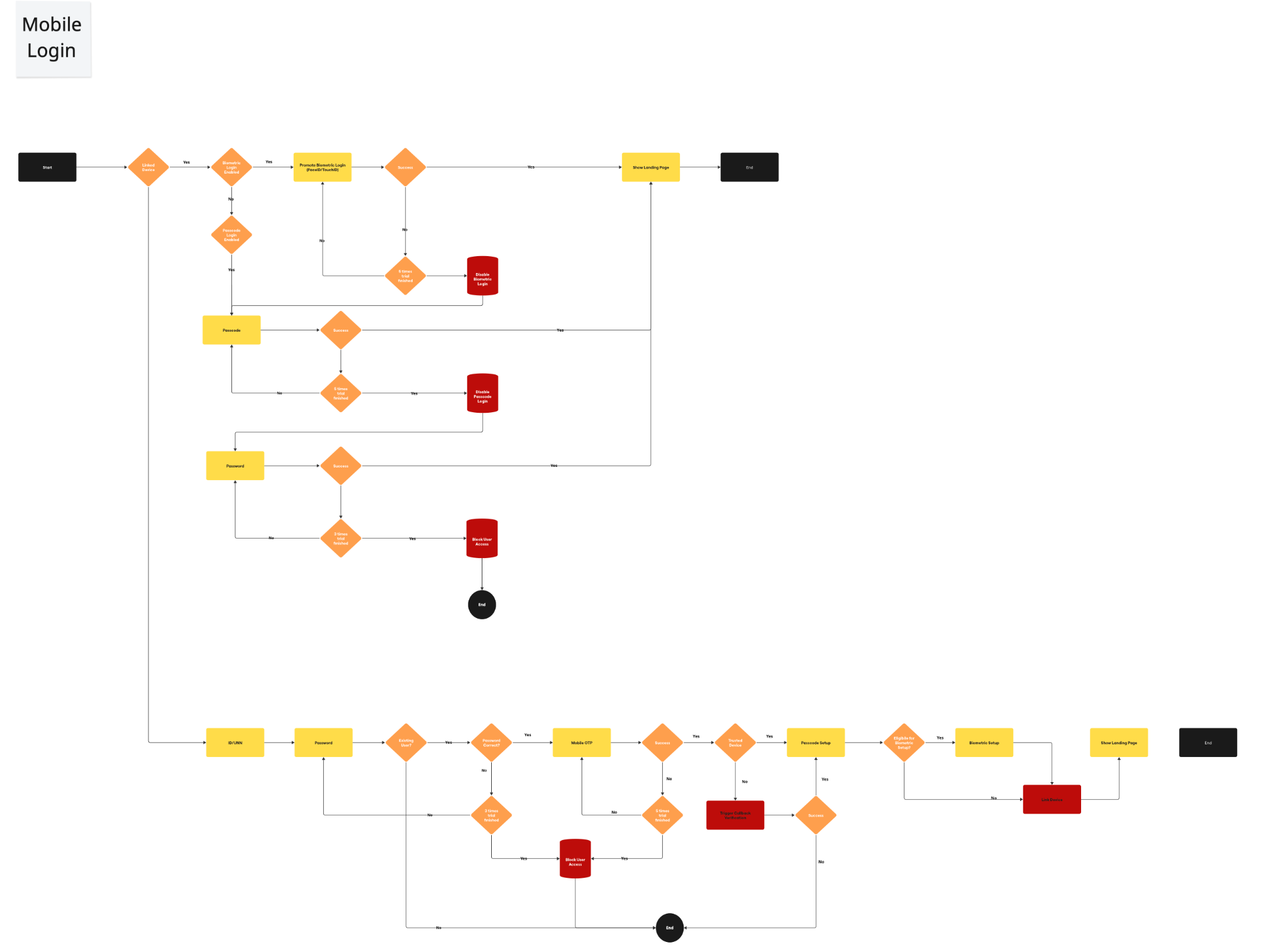
* **Detailed** **log in Flow:**

|  |  |
| --- | --- |
| Step #1 | **Linked Device**  The device is checked to see if it is **linked or not.**   * If the device is **not linked**, you will be taken to a different workflow to link the device (**we will discuss this later**). * If the device is **linked**, you will be taken to the “**Biometric Login Enabled”** step. |
| Step #2 | **Biometric Login Enabled**  Checking whether **Biometric Login is enabled or not**   * If **biometric login is not enabled**, you will be taken to the "**Passcode Login Enable**" step. * If **biometric login is enabled**, the user is asked to enter it, and then checked:  1. If **biometric login is available** (touch or face recognition), they will proceed to the next step, which is the "**Landing Page.**" 2. If **biometric login is not available**, they will be given (5 attempts) to enter it again.  * If **successful**, you will proceed to the next step, the **"Landing Page."** * If **failure,** and all attempts are finished, “biometric login” will be disable, and “**Passcode Login”** will be activated. |
| Step #3 | **Passcode Login**  The user enters the passcode, and it is verified.   * If the passcode is **correct**, the user proceeds to thenext step, which is the "**Landing Page.**" * If the passcode is incorrect, they will be given (5 attempts) to enter it again.  1. If **successful**, you will proceed to the next step, the **"Landing Page."** 2. If **failure,** and all attempts are finished, “passcode login” will be disable, and “**Password Login”** will be activated. |
| Step #4 | **Password Login**  The user enters the password, and it is verified.   * If the password is **correct**, the user proceeds to the next step, which is the "**Landing Page.**" * If the password is **incorrect**, they will be given (5 attempts) to enter it again.  1. If **successful**, you will proceed to the next step, the "**Landing Page.**" 2. If **failure,** and all attempts are finished, the user will be **blocked**, and the process **stop**.  * The account is unblocked via forget password/reregistration. |

* If the device is **not linked**, the following workflow will be executed. (which is similar to the **portal login workflow**)

|  |  |
| --- | --- |
| Step #1 | **ID/UNN number and Password**   * The user enters their ID/UNN number, then their password. |
| Step #2 | **Check the user in the system**   * The system checks this user:  1. If the user **exists** in the system, they move to the next step, "**Password Verification.**" 2. If the user **doesn't exist** in the system, the process stops. |
| Step #3 | **Check the user password in the system**   * In this step, the entered password is verified.  1. If the password is **correct**, the user will proceed to the next step, which is **“Mobile OTP.”** 2. If the password is **incorrect**, the user is allowed to repeat the process (3 times).  * If **all attempts are completed without entering the password correctly**, the user will be blocked, “**Block User Access**” and the process will stop. * If the password is entered **correctly**, the user will proceed to the next step, which is **"Mobile OTP."** |
| Step #4 | **Mobile OTP**   * A 4-digit code will be sent to the user's mobile phone number. * **Example:**  |  |  | | --- | --- | | In English | In Arabic | | **“Please use OTP: 1111**  **For: Login"** | "نأمل إستخدام رمز التفعيل: ١١١١  من أجل: تسجيل الدخول" |  1. If the code is **confirmed** by the user, they will proceed to the next step, **"Trusted Device."** 2. If the code is **not confirmed**, they will only be allowed to repeat the process (5 times.)  * If **all attempts are completed** **without the code being entered correctly**,the user will be **blocked,** “**Block User Access**” and the process will stop. * If the user **successfully** enters the code correctly, they will proceed to the next step, **"Trusted Device."** |
| Step #5 | **Trusted Device**   * The device will be checked to see if it is **trusted or not.**  1. If the **device is trusted**, they will proceed to the next step, "**Passcode Setup"** 2. If the device is **not trusted**, the system will take a **callback** action for the user. "**Trigger Callback Verification**",   \*\*\*\* The voice message contains,  "Dear customer, We have received a login request from a new device. If you are the one initiating this request, press 1, or press 2 for cancellation."  Arabic also:  “عزيزي العميل، لقد تلقينا طلب تسجيل دخول من جهاز جديد. إذا كنتَ أنت من بدأ هذا الطلب، فاضغط على 1، أو اضغط 2 للإلغاء”   * If the callback is **successful** and the user confirms, they will be redirected to the **"Passcode Setup"** * If the callback **fails**, the process **stops**. * The voice message text can be changed. |
| Step #6 | **Passcode Setup**   * The user creates their own passcode and then proceeds to the next step, "**Biometric Setup Verification**" This step is checked.  1. If the user is **eligible to setup biometric**, they proceed to the next step,**"Biometrics Setup"**,and the user enters their biometrics, then proceeds to "**Link Device**" and then to the "**Landing Page.**"   \*\*\*\* A text message notification is sent stating, "A new device has been added as a trusted device."  **Arabic also**  “تمت إضافة جهاز جديد، كجهاز موثوق به”   1. If the user is **not eligible to setup biometric**, they proceed to the "**Link Device"** step and then to the "**Landing Page.**"   \*\*\*\* A text message notification is sent stating, "A new device has been added as a trusted device."  Arabic also  “تمت إضافة جهاز جديد، كجهاز موثوق به” |

* **Log in Process-Flow:**



* Note: You can also access the file via the following link:

[Mobile\_Login\_V1.pdf](https://disholding.sharepoint.com/:b:/s/Holding/ERzMFq43sAxNm8uyyH_XTEMBAPY67ZQuI4p6Ignlwd_aeQ?e=vibgQv)

**3. Forget Password**

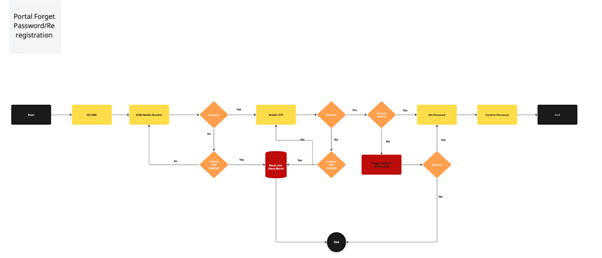
* **For “Portal”**
* **Service Description:**
* If you forget your password or your account is locked due to multiple incorrect login attempts, the “Forgot Password” process allows registered users to securely reset their password through the web portal.
* The primary objective is to verify the user’s identity using their registered mobile number and provide a secure way (such as OTP verification) to allow them to create a new password and regain access to their e-wallet account.
* This process includes verifying:
* ID/DOB number
* UNN/Mobile Number
* Verify ID/UNN
* OTP validation
* Trusted device
* Verify trusted device
* Reset Password
* **General User Story:**

"As a registered user, I want to reset my forgotten password through the **portal** by verifying my identity, so that I can regain secure access to my e-wallet account."

* **Detailed** f**orget password Flow:**

|  |  |
| --- | --- |
| Step #1 | **ID/DOB and UNN/Mobile Number**   * The user enters their ID/DOB or UNN/Mobile Number, then completes their verification.  1. If the user enters it **correctly**, they will proceed to the next step, "**Mobile OTP."** 2. If the user enters it **incorrectly**, they will be given (3 attempts) to re-enter it.  * If **successful**, they will proceed to the next step, **"Mobile OTP."** * If **failure** occurs and all attempts are finished, the user will be **blocked “hard blocked**” and the process will stop. * **Hard block /** This block can only be lifted through a **call center**. The user contacts the call center to have their account **verified** and the hard block removed. |
| Step #2 | **Mobile OTP**   * A 4-digit code will be sent to the user's mobile phone number. * **Example:**  |  |  | | --- | --- | | In English | In Arabic | | "Please use OTP: 1111  For: Password Change " | "نأمل إستخدام رمز التفعيل: ١١١١  من أجل: تغيير كلمة المرور" |  1. If the code is **confirmed** by the user, they will proceed to the next step, **"Trusted Device."** 2. If the code is **not confirmed**, they will only be allowed to repeat the process (5 times).  * If **failure** occurs and all attempts are finished, the user will be **blocked “hard blocked**” and the process will stop. * If the user **successfully** enters the code correctly, they will proceed to the next step, **"Trusted Device."** |
| Step #3 | **Trusted Device**   * The device will be checked to see if it is **trusted or not.**  1. If the **device is trusted**, they will proceed to the next step, "**Set Password."** 2. If the device is **not trusted**, the system will take a **callback** action for the user. "**Trigger Callback Verification**"   \*\*\*\* The voice message contains,  " Dear customer, we have received a password change request from a new device. If you initiated this request, press 1 or 2 to cancel.  Arabic also:  “عزيزي العميل، لقد تلقينا طلب تغيير كلمة مرور من جهاز جديد. إذا كنتَ أنت من بدأ هذا الطلب، فاضغط على 1، أو اضغط 2 للإلغاء”   * If the callback is **successful** and the user confirms, they will proceed to the next step, "**Set Password."** * If the callback **fails**, the process stops. |
| Step #4 | **Set Password**   * The user resets his password, and it is confirmed. |

* **Forget Password Process-Flow:**



* Note: You can also access the file via the following link:

[Portal\_Forget\_Password\_V1.pdf](https://disholding.sharepoint.com/:b:/s/Holding/ET_XlU3kkT9CqVGpH0RR0_oBUpM69rQXsV7_eUrzm_1dsQ?e=uZFZB8)

**4. Forget Passcode**

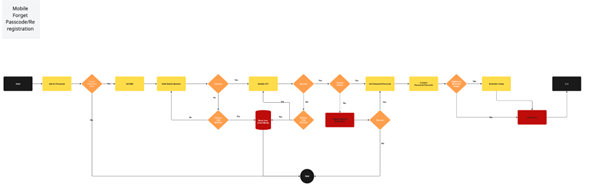
* **For “Mobile”**
* **Service Description:**
* Forgot Passcode is the process that allows a registered user to securely reset their passcode through a **mobile** application.
* The primary objective is to verify the user’s identity using their registered mobile number and provide a secure way (such as OTP verification) to allow them to create a new passcode/password and regain access to their e-wallet account.
* This process includes verifying:
* ID/DOB number
* UNN/Mobile Number
* Verify ID/UNN
* OTP validation
* Trusted device
* Verify trusted device
* Reset Passcode / Password
* Biometric Setup
* Linked device verification
* **General User Story:**

"As a registered user, I want to reset my forgotten passcode through a **mobile application** by verifying my identity, so that I can regain secure access to my e-wallet account."

* **Detailed** f**orget passcode/password Flow:**

|  |  |
| --- | --- |
| Step #1 | **Enter Passcode**   * If the user forgets his **passcode**, we ask him to enter his **password**.  1. If the user also forgot the password, proceed to the **"**I**D/DOB or UNN/Mobile Number" step**. 2. If the user didn't forget the password, the **process** **stops**. |
| Step #2 | **ID/DOB and UNN/Mobile Number**   * The user enters their ID/DOB or UNN/Mobile Number, then completes their verification.  1. If the user enters it **correctly**, they will proceed to the next step, "**Mobile OTP."** 2. If the user enters it **incorrectly**, they will be given (3 attempts) to re-enter it.  * If **successful**, they will proceed to the next step, **"Mobile OTP."** * If **failure** occurs and all attempts are finished, the user will be **blocked “hard blocked**” and the process will stop. * **Hard block /** This block can only be lifted through a **call center**. The user contacts the call center to have their account **verified** and the hard block removed. |
| Step #3 | **Mobile OTP**   * A 4-digit code will be sent to the user's mobile phone number. * **Example:**  |  |  | | --- | --- | | In English | In Arabic | | "Please use OTP: 1111  For: Password Change " | "نأمل إستخدام رمز التفعيل: ١١١١  من أجل: تغيير كلمة المرور" |  1. If the code is **confirmed** by the user, they will proceed to the next step, **"Trusted Device."** 2. If the code is **not confirmed**, they will only be allowed to repeat the process (5 times).  * If **failure** occurs and all attempts are finished, the user will be **blocked “hard blocked**” and the process will stop. * If the user **successfully** enters the code correctly, they will proceed to the next step, **"Trusted Device."** |
| Step #4 | **Trusted Device**   * The device will be checked to see if it is **trusted or not.**  1. If the **device is trusted**, they will proceed to the next step, "**Set Password / Passcode."** 2. If the device is **not trusted**, the system will take a **callback** action for the user. "**Trigger Callback Verification**"   \*\*\*\* The voice message contains,  " Dear customer, we have received a password change request from a new device. If you initiated this request, press 1 or 2 to cancel."  **Arabic also:**  “عزيزي العميل، لقد تلقينا طلب تغيير كلمة المرور من جهاز جديد. إذا كنتَ أنت من بدأ هذا الطلب، فاضغط على 1، أو اضغط 2 للإلغاء”   * If the callback is **successful** and the user confirms, they will proceed to the next step, "**Set Password / Passcode."** * If the callback **fails**, the process stops. |
| Step #5 | **Set Password / Passcode**   * The user resets his Password / Passcode and then confirms it. * The device will be checked to see if it is eligible for biometric setup or not.  1. If the device **accepts biometrics**, the user will be directed to the “**Biometric Setup”**, where they will enter their biometrics and then proceed to **“Link device”**, where the device will be **linked**. 2. If the device **doesn't accept biometrics**, the user will be directed to **“Link device”**, where the device will be **linked**. |

* **Forget Passcode/Password Process-Flow:**



* Note: You can also access the file via the following link:

[Mobile\_Forget\_Passcode\_V1.pdf](https://disholding.sharepoint.com/:b:/s/Holding/ESFktgrcje1Gj8Wp3m1N-usBfcQo8ZXmMBSpaurjWNuguw?e=0feYBI)

**5. Change Mobile Number**

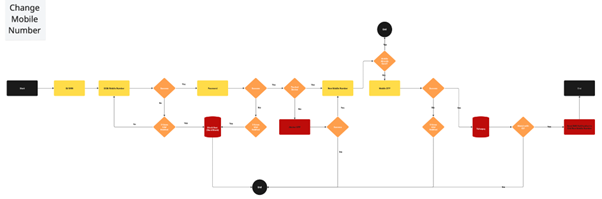
* **Service Description:**
* Changing an old mobile number due to the user losing it for any reason is a process that allows the registered user to update their mobile number and then link it to the e-wallet.
* The main objective is to verify the user's identity and authenticate the new mobile number using secure verification methods, such as Absher OTP verification and then Mobile OTP verification, to ensure the accuracy and validity of the updated contact information before implementing the change in the system.
* This process includes verifying:
* ID/DOB and UNN/Mobile Number
* Verification
* Verify password
* Verify trusted device
* Absher OTP
* OTP Mobile
* Tahaquq Service
* Notification
* **General User Story:**

"As a registered user, I would like to **change my old phone number** associated with my e-wallet account to a new one, so that I can receive all notifications, (OTP) and account-related communications on my new number."

* **Detailed** c**hange mobile number Flow:**

|  |  |
| --- | --- |
| Step #1 | **ID/DOB and UNN/Mobile Number**   * The user enters their ID/DOB or UNN/Mobile Number, then completes their verification.  1. If the user enters it **correctly**, they will proceed to the next step, "**Password".** 2. If the user enters it **incorrectly**, they will be given (3 attempts) to re-enter it.  * If **successful**, they will proceed to the next step, **"Password."** * If **failure** occurs and all attempts are finished, the user will be **blocked “hard blocked**” and the process will stop. * **Hard block /** This block can only be lifted through a **call center**. The user contacts the call center to have their account **verified** and the hard block removed. |
| Step #2 | **Password**   * The user enters the password, and the entered password is verified.  1. If the password is **correct**, the user will proceed to the next step, which is **“Trusted Device.”** 2. If the password is **incorrect**, the user is allowed to repeat the process (3 times).  * If the password is entered **correctly**, the user will proceed to the next step, which is **"Trusted Device."** * If **failure** occurs and all attempts are finished, the user will be **blocked “hard blocked**” and the process will stop. |
| Step #3 | **Trusted Device**   * The device will be checked to see if it is **trusted or not.**  1. If the **device is trusted**, they will proceed to the next step, "**New Mobile Number."** 2. If the device is **not trusted**, they will proceed to the next step. "**Absher OTP**" |
| Step #4 | **Absher OTP**   * Because the system can't send a message to the user's old mobile number, this service (**Absher**) sends an OTP to the user's mobile number registered with the Ministry of Interior (Absher). * The OTP is then checked: * If the user enters it **correctly**, they will proceed to the next step. **"New Mobile Number."** * If the user enters it **incorrectly**, the process will stop. |
| Step #5 | **New Mobile Number**   * The user enters the **new mobile number**, which is then verified.  1. If the number **exists** in the system, the process will be stopped. 2. If the number **doesn't exist** in the system, the process will proceed to the next step, "**Mobile OTP**."   **Acceptance Criteria:**   * The user must enter a valid local Saudi phone number that starts with (05) and consists of exactly 10 digits (numbers only, no letters), with support for both Arabic and English numerals. * The system automatically converts Arabic numerals to English. * The system must verify that the phone number is not already associated with another user account. * The system must display the digit keypad only for the customer. * The user cannot proceed to the OTP verification step unless a valid number is entered. A clear error message must be displayed if the input is invalid or incomplete.   **Negative Scenarios**   * Invalid Format:   Incorrect or incomplete number → "Please enter a valid phone number."   * Empty Field:   No input provided → "This field is required."   * Duplicate Number:   Number already used → "The phone number is already in use."   * Too Many Attempts:   5+ rapid attempts → "Temporarily blocked. Try again later."   * System Error:   Server failure or internal error → "A system error has occurred." |
| Step #6 | **Mobile OTP**   * A 4-digit code will be sent to the user's mobile phone number. * Example:  |  |  | | --- | --- | | In English | In Arabic | | “Please use OTP: 1111  For: Change Mobile Number" | "نأمل إستخدام رمز التفعيل: ١١١١  من أجل: تغيير رقم الجوال" |  1. If the code is **confirmed** by the user, they will proceed to the next step, **"Tahaquq."** 2. If the code is **not confirmed**, they will only be allowed to repeat the process (5 times).  * If the user **successfully** enters the code correctly, they will proceed to the next step, **"Tahaquq."** * If **failure** occurs and all attempts are finished, the process will stop. |
| Step #7 | **Tahaquq Service**   * Tahaquq service that links the user's entered mobile number with the ID number.  1. If there is a **match** between the **mobile number and the ID number**, a **notification** will be sent that says:  |  |  | | --- | --- | | In English | In Arabic | | Dear customer, your mobile number has been successfully changed from {xxx1234} to {xxx1234} | عزيزي العميل، تم تغيير رقم جوالك من {xxx1234} إلى {xxx1234} بنجاح. |  1. If there is no match, the process is stopped. |

* **Change mobile number Process-Flow:**



* Note: You can also access the file via the following link:

[Change\_Mobile\_Number.pdf](https://disholding.sharepoint.com/:b:/s/Holding/EatvXVQwT6ZFhjB3cuHdpSEBNFBrZeWtfQQQm8gbZdoNTg?e=1vncpv)