

INTERNET BANKING APPLICATION (Personal)

**CUSTOMER DETAILS**

FOR BANK USE ONLY - No.: \_\_\_\_\_

Surname: \_\_\_\_\_ First name: \_\_\_\_\_

User ID: \_\_\_\_\_ (Choose your User ID - Min 6 alpha-numeric characters)

Service Type: Transact  View only

Email Address: \_\_\_\_\_

Mobile Number: \_\_\_\_\_ - \_\_\_\_\_  
(country and regional code) (mobile number)

PIN to be communicated by: Post  Email \*

**PIN**

- 🔔 DO NOT DISCLOSE your Password to anyone and DO NOT RECORD it in a way that can be easily copied.
- 🔔 Note that you will be requested to change your password on your first login. If this is not the case, please notify the Bank immediately.
- 🔔 Your password is highly confidential. Bank officers will never ask for your password. In no circumstances should you communicate your password to the Bank officers.
- 🔔 Please notify us immediately if you believe your password has been compromised.
- 🔔 You are solely responsible for securing and maintaining the confidentiality of your password.

**\*PIN BY EMAIL**

The Customer authorizes the Bank to send the PIN by email to the address mentioned above at the Customer’s own risk and peril and the Bank will not be held responsible for any prejudice or loss suffered by the Customer. The Customer must keep the Bank indemnified at all times against all proceedings, claims, loss, damage and expenses which may be brought against the Bank or suffered or incurred by the Bank and which have arisen, directly or indirectly, from the Bank accepting to send the PIN by email. Please DO NOT REPLY or FORWARD the email sent by the bank. PLEASE DELETE this email from your mail box once you have memorized your password.

**One Time Passwords**

One-Time-Password for Login will be sent by: SMS  Email \*\* WhatsApp \*\* Google Authenticator \*\*

One-Time-Password for Transaction will be sent by: SMS  Email \*\* WhatsApp \*\* Google Authenticator \*\*

**\*\*One Time Passwords by Email**

For customer security reasons, the Bank recommends that OTPs only be transmitted by SMS to the Customer’s mobile number held on the Bank’s records. If for any reason, the Customer should opt for OTPs to be transmitted to the Customer’s preferred channel (Email, WhatsApp or Google Authenticator) whether in addition to, or instead of SMS OTPs, the Customer’s attention is drawn to clause 12 of the attached Terms and Conditions.

**Agreement**

I confirm that the information in this Application is true and correct and I agree to be responsible for all transactions through the internet banking services. I confirm having read and understood all the rules relating to the Bank’s internet banking services, including the User Agreement, the Bank’s General Terms and Conditions (both accessible through the Bank’s website) and the attached terms and conditions.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

## TERMS & CONDITIONS

1. The registration, activation or use of the One Time Password (OTP) by the Customer will constitute conclusive evidence of the Customer's acceptance to these Terms and Conditions.

2. The OTP is a unique and time-sensitive password used as added security on Internet banking. The OTP does not replace the password (PIN) the Customer uses to log on to Internet banking but provides an additional layer of security. The OTP facility is a service provided by the Bank to its customers to protect the use of Internet banking by the Customer by requiring the Customer to verify his/her identity using an OTP. The OTP will be transmitted to the Customer's contact details held by the Bank for such purpose. The purpose of the OTP facility is to protect the Bank's customers, including the Customer, by reducing the risks of unauthorised account access, identity theft and fraud.

3. The Bank reserves the right to modify or suspend, temporarily or permanently, the OTP, with respect to the Customer or all its customers, with or without notice, where the Bank considers it necessary or advisable to do so, including when the Bank suspects breach of security, or when the Bank has reasonable grounds to suspect that the Customer's registration data is inaccurate, incomplete, or when the Bank needs to suspend the OTP facility for maintenance or other reasons. Any transactions conducted using the OTP facility prior to its suspension will remain valid and the Customer will continue to be bound by these Terms and Conditions in respect of such transactions.

4. Activation - The Customer must comply with any activation procedures that the Bank may from time to time prescribe in order to use the OTP facility.

5. Accuracy of information - The Customer must promptly update his/her contact details, to keep them accurate, and complete, and upon request provide such additional contact details to the Bank as the Bank sees fit.

6. After the registration and activation of the OTP facility, the Customer will be provided with an OTP when effecting an internet banking transaction. If the Customer is unable to insert the OTP provided by the Bank, within the prescribed period of time, or if the authentication through the OTP facility otherwise fails, the Customer will not be able to effect any transaction.

7. Internet Banking Session Timeout - To protect customer information when using Internet banking, the Bank will require the Customer to choose a session timeout duration. If the Customer is idle during a time period greater than that duration, the Customer will be logged out of the internet banking portal automatically. The session timeout duration is chosen by the Customer. The Customer assumes all risks associated with his/her selection.

8. The Customer may be late in receiving or may be unable to receive the OTP due to the various reasons, including the following:

- issues with mobile or other electronic device (including loss of device);
- issues with mobile or internet network or service provider; or
- change in contact details without having informed the Bank.

The Bank is not liable for any service charge levied by a mobile or internet service provider in connection with the OTP or for any issue with the mobile or internet network or service provider.

The OTP will only be sent to the Customer's contact details registered with the Bank for such purpose.

9. Customer security duty - The Customer agrees and undertakes to act prudently and in good faith when using the OTP facility. The Customer will be solely responsible for maintaining the confidentiality of the OTP and for any transaction involving the use of the OTP facility. The Customer must not disclose to any other person or otherwise permit or enable any other person to obtain any OTP.

10. The Customer must immediately notify the Bank of any suspected or actual unauthorized use of his/her OTP.

11. Liabilities and obligations of Customer - The Bank will not be liable for any loss, damage, interruption, delay or non-performance arising out of the Customer's use of the OTP facility or any delay or non-delivery of an OTP, and the Customer agrees to indemnify the Bank in each of these instances. The Customer will be liable for all transactions conducted through Internet banking, with/without the OTP, and whether such OTP was transmitted to the Customer via email or SMS. The Customer is fully liable for all claims, losses and consequences arising out of or in connection with the use of the OTP facility. The Customer confirms that it has taken full responsibility and assumes all liability for fraud, identity theft or unauthorized account access in connection with the OTP facility and the Bank's internet banking services generally.

12. The Customer agrees that the Bank may use, hold, store and/or process, by computer or otherwise, in any location whatsoever, any information given by the Customer in dealings with the Bank, or obtained by the Bank in connection with the OTP and any information relating to the Customer's accounts. The Bank will disclose data only if the Bank has obtained the prior written consent of the Customer, or has a right or duty to disclose.