Remote Banking Terms and Conditions

This agreement applies to you if you use any of the following self-service banking channels: Online Banking, FNB Banking App, FNB .Mobi or Cellphone Banking. This important document sets out the rights and duties between you and First National Bank Swaziland Limited, with registration number 24/1988 ("the bank"). Please read this document carefully. If you do not understand any part of this document you must contact the bank for further clarification. This document was last updated on 05 October 2016.

It forms an agreement between First National Bank Swaziland Limited ("the Bank") and the Bank's customer and if applicable, those natural persons the customer has chosen to access and/or transact on its accounts, using the service channels ("users"). For convenience, in this agreement "you" or "your" refers to both "the customer and user(s), or the customer or a user, as the context requires" and (where appropriate) also refers to any separate legal entity, such as a company. In this agreement "we, us, or our" only refers to the Bank. This agreement governs your and our rights and obligations when you use any of the service channels. You will become bound to the most recent version of this agreement when you register to use any of the service channels; obtain access rights; access mechanisms and/or access codes to use any of the service channels; or when you use any of the service channels, whichever happens first. Before you can use the service channels you must register on the service channel

This agreement also applies to any person(s) the account holder appoints to use the service channels on their behalf (e.g. to do transactions on their accounts). In this agreement these persons are called authorised users.

In this agreement, the following words will have the following meanings:
The words "you" or "your" means the account holder and their authorised users. The words "us", "we", or "our" only means the bank. Before you can use the service channels, you must register on the service channel. For more information on how to register for the different service channels please refer to www.fnbswaziland.co.sz.

If you are younger than 21, you must get your parent or legal guardian's consent to use the service channels, unless you have been emancipated. "Emancipated" means the court has given you the right to act without your parent or guardian's consent.

When does this agreement start?

This agreement starts as soon as any of the following happens:
- When you register to use any of the service channels.
- When you get access to be able to use any of the service channels.
- When you actually use any of the service channels.

Other terms & conditions that also apply to you

This agreement applies along with other terms & conditions of the bank that govern your accounts, our services and our relationship with you.
Certain of the products and services that we make available to you on the service channels also have their own terms and conditions. If applicable, see:
- Prepaid products: See MTN Network Operator terms & conditions that apply to prepaid products like airtime purchases.

You must read this agreement together with the other relevant terms & conditions. If there is a conflict (difference) between this agreement and any other product terms & conditions, the provisions of the other product terms & conditions will apply. If the conflict relates to the use of the service channel, this agreement applies.

You must comply with any user guidelines we publish on the service channels

For your protection and to ensure that the service channel works correctly, you must comply with the user guidelines we put on the service channels from time to time. If there is a conflict (difference) between this agreement and the guidelines, this agreement will apply instead of the guidelines.

How we make terms & conditions and other information available to you

From time to time we may include hyperlinks to terms and conditions ("Terms") on the service channels. Where it is not possible to use a hyperlink, we may refer to the Terms on the service channels. You must follow our instructions or the hyperlink and read the Terms, as they form part of the agreement between you and us. If the service channel you are using does not enable you to access the Terms via a hyperlink for any reason, you must visit our website, our branches or contact us (contact details are available on the website) or follow our instructions to get a copy of the Terms. Any Terms & Conditions we refer to are important. You must read them carefully because they contain important contractual information. Due to space constraints on some channels we sometimes only refer to terms & conditions as "T&Cs".

Fees you must pay to use the Service Channels

The fee you must pay includes a services fee for use of the service channel and a transaction fee for the transactions you do on the service channel. For more information about the service channels fees that you must pay to use the service channel please refer to our

You are responsible for making sure you have the necessary equipment and software to use the service channels

To be able to access the service channels you must have the necessary hardware, software and access to third-party communication services. You will be responsible for applying the cost of this and the cost of any upgrades that you require. To access Online Banking you need to have access to a computer that has an active an account with an Internet Service Provider (ISP) and an Internet browser software program. To access Cellphone Banking you need to be activated via your cellphone and cellphone network service provider. We have no control over the equipment, software or service providers. We are not responsible for any error or delay that may arise as a result and are also not responsible if you are unable to access the service channels because of your equipment, software or services provided to you by third parties.

The *inContact* Service is a messaging system which provides you with notifications of certain account activity via SMS to your selected Mobile number and/or email to your email address and/or, IM (Instant Message) to linked Banking App. Should you elect to receive your inContact notifications via your Banking App be advised that we will first attempt to send you an IM and should we be unable to do so, we will send you an SMS.

Customers who have a linked Banking App will not receive an OTP via sms but a notification via IM (instant messaging) via the Banking App requesting you to approve or decline the transaction. It is your responsibility to ensure that you are connected to WiFi or have data on your device.

For your protection and security you must enter the correct access information to identify yourself whenever you use or logon to the service channels

Since we deal with each other in a non-face to face environment, for your security you will need to enter the correct access information or take any other steps acceptable to us for us to verify your identity and the electronic communications you send us using the service channels each time you logon to the service channels. This is known as "verification". Access information, includes any physical devises we give you to allow you to logon to the relevant service channels like your Cellphone Banking PIN. All electronic communications that are sent to us after you have met our verification requirements during logon will be treated as valid and authentic. This means that these electronic communications will have the same legal effect as written and signed paper communications from you. To protect you, we can refuse to act on any instructions you send us or can cancel your access (temporarily or permanently) if you don't meet the verification requirements. This includes where you enter the wrong access codes.

We are entitled to act on and accept all transactions done after your access codes have been entered or applied

Since we deal with you non-face-to-face we will act on and accept all instructions or transactions ("transactions") done after your correct access codes have been entered and you meet the verification requirements set by us. We will assume that all such transactions have been authorised by you, even if such transactions took place without your knowledge or consent or were not authorised by you. This will not apply to transactions that occur after you have requested that we cancel your access codes.

Authorised Users act on your behalf as your agent

By allowing an authorised user to access your account using the service channel, you give that person the authority to act as your agent. This means that anything the authorised user does or doesn't do will be attributed to you. In other words their actions or failure to act (omission) will be considered by us as your actions or failure to act (omission).

We may require of an additional layer of security (verification) for certain transactions. Such as where a unique number (OTP or one time PIN) is sent to your device before the transaction can be completed. Take note: You can have the OTP sent to your inContact number or a separate mobile number of your choice. **A loss of signal to your OTP or inContact number can indicate a SIM SWAP and you should check your account immediately or notify the Bank to minimise your loss**.

Take note: For your convenience, the same login or access details can be used to access different electronic channels. This means that if your access details or lost or stolen or disclosed to someone else "compromised" your details on one channel you can be defrauded across all the electronic channels which can expose you to greater losses. **You must immediately contact the Bank if you know or even suspect that your access details have been compromised to ensure that your loss is minimised.**

We are entitled to act on and accept all transactions done after your access codes have been entered or applied
Since we deal with you non-face-to-face we will act on and accept all instructions or transactions ("transactions") done after your correct access codes have been entered and you meet the verification requirements set by us. We will assume that all such transactions have been authorised by you, even if such transactions took place without your knowledge or consent or were not authorised by you. This will not apply to transactions that occur after you have requested that we cancel your access codes.

Steps you must take to protect your access information (access codes, cards and equipment)

Your access information is the only way we can know you are who you say you are when you transact, you must keep your access information secret and safe and you must not allow anybody to use your access information. **You must never give or show your access information to any person, including any person who is an employee of the bank or claiming to work for or represent us in any way. You must never respond to requests to enter or "confirm" your access codes, sent to you via an email, SMS or instant message. This is known as "phishing" where the sender tries to trick you into giving them your confidential information by pretending a communication was sent from us. The bank will NEVER ask you to give us your sensitive secret information including access codes by email, SMS, instant message or even over the telephone. If you respond to these "phishing" messages and lose money as a result of doing so, the bank will not refund you. If you respond to these "phishing" messages and lose money as a result of doing so, the bank will not refund you.** If you receive suspicious communications (including emails, SMSs) call the bank's fraud team +268 251 84637 or after hours on +27 11 369 1189 or send an email to: callcentreswz@fnb.co.za. Please include your name and number in your email in case we need more information from you.

You must not keep your access codes together with other banking documents. Do not store your access codes on the equipment you use to access the bank service channels. For example, never store your PIN or Cellphone Banking PIN on, with or near your cellphone, computer, or on your smart phone. For security purposes, we recommend that you memorise your access codes. You must also follow the tips published on the bank's Security Centre or Online Banking Communications Page. You are not allowed to register for the service or access the service channel using someone else's access information or personal information.

Steps you must take to protect yourself

NOTE: *information that is sent over an unsecured link or communication system can be unlawfully monitored, intercepted, or accessed. While we take all reasonable steps to prevent this from happening, you need to understand that this risk exists.*

You play an important role in protecting yourself against fraud. For your safety you must follow the security tips/recommendations we give you on the service channels from time to time. You must also read the tips published at the bank's Security Centre and the online banking Communications Page. You must (where applicable) log off from the service channel when you have finished transacting. The bank recommends that you do not use public communication facilities such as internet café's, but when you do, you must take special care. You must use our recommended hardware and software. This includes security software that is recommended by us. Please refer to the bank's Security Centre and Online Banking Communications Page for more information. Failure to use the recommended hardware and software may result in the service channel not being available or not operating properly or may also expose you to a greater security risk.

Cellphone Banking Customers

- If you are a cellphone banking customer and you notice anything suspicious you must also contact your service provider/network operator to report the suspicious behaviour e.g. SIM Swaps:
  MTN +268 76068999 or +268 2406 0000

You must IMMEDIATELY ask us to cancel your access code(s) if you suspect or know that your access code(s) have been lost, stolen or may be used without your permission.

Prompt notification is the best way of keeping your losses to a minimum and you must tell us immediately if you suspect or know that your access information has been lost, stolen or compromised (might be used without your permission). You must notify us immediately if your cellphone is lost or stolen and ask us to delink your cellphone from your online banking profile. In instances whereby you suspect or know that your access code(s) have been lost, stolen or may be used without your permission, immediately call the bank's Fraud Team on +268 251 84637 or out of hours to our Johannesburg Call Centre on +27 11 369 1189.

If there is a dispute about whether or when you told us to cancel your access code(s), it will be your responsibility to prove how and when you told us to cancel your access code(s). For this reason you must keep any reference numbers we give you when you call us to cancel your access code(s). We advise you to request a reference number and store it for every call you make to us.

After we have cancelled your access code(s) we will reject all transactions done from the date on which your access code(s) were cancelled. If possible we will also temporarily stop or reverse instructions that we received but which we have not yet processed before your access code(s) were cancelled, however we cannot guarantee that this will be done.

We reserve the right to block your access to the service channels at any time to maintain or restore security if we reasonably believe that your access code(s) have been or may be obtained or are being used or may be used by an unauthorised person(s).

What you must do if you suspect or know about fraud on your account?

We strongly recommend that you ensure that your device which you use for transacting is always in your possession and protected with an additional access code, password or pattern lock. We further advise that should your device to which your Banking App is linked is no longer or in your possession either permanently (for eg. Due to theft, loss or in the event that you have sold it) or temporarily (your device is being repaired) you should delink your Banking App immediately.

If you receive suspicious communications (including emails, SMSs) call the Bank's Fraud Team on 25184637 (dialling code +268).
For immediate action and assistance, we recommend that you call the Fraud Team. Please include your name and number in your email in case we need more information from you

Note: This section does not apply if the fraud or suspected fraud was committed by authorised users (persons who have been authorised by the account holder to transact on the account holder's behalf).
You must tell us immediately when you become aware that a suspicious transaction has taken place and you must open a case at the nearest Royal Swaziland Police (RSP) office. We will investigate any loss that you suffered because of the alleged fraud. You must co-operate with us and the RSP in any investigation. We may opt to pay you back at our discretion once it has been established that you suffered financial loss as a direct result of the fraud if the following conditions are met:

- You have followed the safety tips we recommended and have complied with your duties under this agreement , in particular, those mentioned to you above as 'Steps you must take to protect your access information (access code(s), cards and equipment' and 'steps you must take to protect yourself'
- Your account was registered for the InContact notification service and you were actively using the service when the fraud occurred.
- You have not compromised your PIN or your MOPIN.

Cancelling the Access Code(s) of Authorised Users - You must tell us in writing if an authorised user's access rights must be changed or cancelled

When an authorised user is no longer allowed to transact on your account you/we have the right to demand that they return any physical devices we gave them to enable them to transact. When you as the account holder takes back the authorised user's physical access device you must notify us in writing or via the Call Centre or your branch that the authorised user's access rights must be cancelled, and the card or device must be destroyed or returned to us. The account holder is not allowed to use any authorised user's access code(s). For your security, the access code(s) must be cancelled. We will issue new authorised users with new access information.

You must notify us immediately when any user's access rights must be changed or cancelled by completing and signing this required mandates/bank form(s). This can also be done by yourself on the website within your Online Banking platform. Any cancellation of, or change to a user's access rights will not affect any instruction submitted by that user before the change has been made.

Cellphone Banking Customers agree that the bank can get their cellphone number from their network operator

If you are a cellphone banking customer you agree that the bank can get your cellphone number from your cellphone network operator. This is done to assist the bank to identify you. For your protection, the bank can (but does not have to) use your cellphone number to identify you.

We respect your privacy. Read our privacy policy for more information

Please read our Privacy Policy published on the website. Our privacy policy explains how, why and when we collect, use, share and store your personal information. Our privacy policy forms part of this agreement with you.

We may monitor your use of the service channels and record our conversations with you

For security purposes, to maintain the proper functioning and safety of our systems and the service channels, or to investigate or detect any unauthorised use of the service channel or our systems, or when the law requires us to do so, we may monitor and record communications or traffic on the service channel.

Certain information, including your account balance information, may be delayed

Certain information, including your account balance information that is made available to you on the service channels may be delayed and may not show your recent transactions. You can confirm your account balance information by contacting us.

We cannot act on or process your instructions unless you have enough money in your account

Any instructions we receive from you on the service channels, including an instruction to pay a third party or transfer money between your accounts will only be carried out if you have enough money in your account or credit in your overdraft facility.

Transaction limits apply to transactions done on the service channels

These limits apply whether these were set for your account for the authorised user or for the service channel itself. Transaction limits are there for your protection. Because of this we will not be able to carry out any instruction from you if you have exceeded your transaction limit or if a transaction will result in you exceeding your transaction limits. If you need to exceed any limits you need to arrange with us for this beforehand. You can do this by visiting your nearest branch. Please contact our call centre to find out what the transactional limits are on our service channels. Each service channel has its own limits.

You are responsible for giving us correct and complete information and instructions when you transact

You are responsible for giving us correct and complete information and instructions when you transact. Unfortunately we are unable to and do not check or confirm any information. **We do not verify the identity or bank account details of the person / entity you are paying and do not compare the account number against the details of the person / entity you are paying, therefore it is your responsibility to make sure that the information you give us is correct. We will not be responsible to the person or entity you are paying for any loss or damage you suffer because you gave the incorrect or incomplete information. We are not responsible if you do not complete an instruction or if you do not follow our instructions when transacting.**

Certain transactions cannot be reversed or stopped once you send them to us

Certain transactions cannot be reversed or stopped once you send them to us, for example, when you buy pre-paid products.

How long does it take to process transactions?

Unless we say otherwise (whether on the service channel or anywhere else), all transactions will be completed in the same amount of time that they generally take to be completed when you perform them at the branch or ATM. Some transactions take longer. It can take up to 2 (two) business days for money to reach persons you are paying by EFT (electronic funds transfer) via the service channels. Please read the guidelines and notices published on the service channel from time to time or contact us to check on the turnaround times especially if your payment is urgent.

How do I know if the bank has received my instruction?

You must not assume that we have received an instruction until we have specifically confirmed that we received that instruction, or acted on that instruction, whichever happens first. **If you are not sure if a transaction has been sent or received or processed you must contact us. You must not submit an instruction again as this can result in the same transaction being processed again. Should this happen you will be responsible for such duplicated transactions**. Messages sent by us of an "automated nature" or messages that were sent using auto response software or programs must not be regarded as a response or confirmation.

Nothing on the service is an offer or professional advice to you

Unless we actually make an offer to you, all material on the service channels is only an invitation to you to do business with us. Nothing on the service channel is given as advice or an offer which is meant to get you to buy or sell anything, or enter into any investment or transaction.

Availability of the service channels. The service channels may not be available from time to time. You must use our other banking channels during this time

You can access the service channels seven days a week, 24 hours a day. However, at certain times, some or all of the service channels or services on them may not be available due to routine maintenance or emergency repairs or because of circumstances outside our control, such as electricity outages/blackouts, or the unavailability of any telecommunication system or networks. In this case you must use our other available banking channels and take reasonable steps to minimise or prevent loss or risk to you. If we need to change the scope of our services, we will try to give you prior notice of such interruptions and changes, but we cannot guarantee that such notice will be given to you. We may stop providing the service channels or any services provided on the service channels at any time. We will however, notify you of this within a reasonable time of these changes being made. You agree that a notice published on the website or a notice sent to you via an email, an SMS or via post will be sufficient notice to you. You will be regarded as having accepted all transactions and changes to your account settings made via the service channels unless you notify the bank of your objection within 5 (five) hours of receiving a notification from us, by any means, including inContact.

Notification Services

If you use notification services such as inContact then the terms & conditions that govern inContact will also apply to you.

The inContact Service is a messaging system which provides you with notifications of certain account activity via SMS to your selected Mobile number and/or email to your email address and/or, IM (Instant Message) to linked Banking App. Should you elect to receive your inContact notifications via your Banking App be advised that we will first attempt to send you an IM and should we be unable to do so, we will send you an SMS.

Customers who have a linked Banking App will not receive an OTP via sms but a notification via IM (instant messaging) via the Banking App requesting you to approve or decline the transaction. It is your responsibility to ensure that you are connected to WiFi or have data on your device.

We are not responsible for links to third party sites, its content or for the third party's actions or omissions, or its goods or services

For your convenience only, the service channels may allow you to view or access third party websites or content or purchase content, products or services provided by third parties. Even though we may make third party websites, content or products or services available to you, we do not endorse or recommend the third party or its products or services. You alone are responsible for deciding whether the third party or its products or services meet your requirements. Terms and conditions and rules may apply to those products and form an agreement between you and the third party. You alone are responsible for obtaining the terms and conditions or rules that apply to you and the products or services offered by the third party.

The bank is not responsible for third party software

From time to time we may make third party software applications ("software") available for download via the service channel. You download and use the software at your own risk. We make no warranty about the software, whether expressed or implied. You will be bound to the licence terms of the software licensor. You hereby indemnify us and hold us harmless if you breach the licence conditions bound to the license terms of the software licensor. You hereby indemnify us and hold us harmless if you breach the licence conditions.

You are responsible for paying the relevant cellphone network service provider charges that you incur when using the service channel. In order to use the Banking App you must ensure that you have a compatible smartphone and access to data. In order to make use of Online Banking or dot.mobi you require a compatible device and access to an internet connection.

We have no control over the equipment, software or service providers. It is your responsibility to ensure that you have the necessary antivirus or anti-malware software on your device. We are not responsible for any error or delay that may arise as a result and are also not responsible if you are unable to access the service channels because of your equipment, software or services provided to you by third parties.

IMPORTANT: FNB's liability will be limited for loss caused by use of the service channels

The bank undertakes to ensure to the best of its ability that the service channels are provided to you in a secure and reliable manner. The bank shall take reasonable care to prevent harm and loss to you. Although the bank takes reasonable care to prevent harm or loss to you, the bank will not be liable for any kind of loss or damage you may suffer, including direct, indirect, special, incidental or consequential damages, because of your use of, or inability to use, the services. This will not apply where the loss/damage arose because of the bank's negligence or intent. In addition to the above the bank is not liable for the following (except where such loss or damage is caused by the Bank's negligence or intent):

- **any loss or damage, which you or any other party may suffer due to unauthorised interception and/or monitoring ;**
- **any loss or damage if you didn't take reasonable steps to safeguard the account, the access codes and/or follow the steps recommended by the bank from time to time;**
- **late or delayed transactions;**
- **loss or damage arising from the unauthorised use of the service channel including where a user exceeds their authority;**
- **the bank is not responsible for any errors or delays in communication systems outside of its control.**

We own the intellectual property rights in the service channel and its content

The contents of the service channels, including all registered and unregistered trade marks, is owned by us and are our intellectual property rights. You may not copy, reproduce, display or use any intellectual property in any manner whatsoever without our prior written consent. Nothing on the service channels must be seen as granting any licence or right of use of any intellectual property. You may not

establish any connection, including via a hyperlink, frame, meta tag or similar reference, whether electronically or otherwise to any part of the service channel or the bank's website without our prior written consent.

How we will communicate with you

You agree that we can send you information about the service channels or this agreement by any means, including but not limited to publishing a notice on the service channel itself or using electronic means, including SMS or email.

We can change this agreement at any time

We have the right to change this agreement or add new terms and conditions for the use of the service channels or value added services at any time. Whenever we change this agreement we will electronically update this agreement. We will notify you of these changes. The use of the service channels will be taken as an acceptance of the agreement. If you do not agree to the changes, you have the right to end this agreement before the end of 7 (seven) days after the changes take effect. If you do not notify us of your intention to end the agreement within this 7 (seven) day period, we can assume that you have accepted the amended agreement or new terms and conditions. A certificate made by the relevant bank's employee, whose authority to do so doesn't need to be proven, will be the proof of the version of the agreement that applies to you.

Ending this agreement

We can end this agreement at any time or end your right to use the service channels, after giving you reasonable notice. This will not affect instructions given to us using the service channels before the agreement ended.

We can also end this agreement and your right to use the service channels immediately if any one or more of the following happens:

- If you commit fraud or we suspect you have done so.
- If we believe that your behaviour was inappropriate or constitutes misconduct.
- If you breach this agreement.
- If you no longer have access to the equipment or services necessary to use the service channels. E.g. Cellphone Network Service Provider removes your registered cellphone number from its network or ends your contract.
- If your account is closed.
- If the law requires us to do this.
- If you don't use the service channel for a period of 6 (six) months or more. If we end the agreement because of this the accountholder will have to register again.

You may end this agreement by notifying us in writing or by phoning our call centre. If you or we end this agreement you will still be responsible to us for all transactions, instructions and fees.

NOTE: It is your responsibility to cancel any scheduled top ups and any recurring services or payments you set up on the service channel. The service channel is just a means of setting up scheduled top ups and recurring services, ending the agreement does not mean these scheduled top ups or recurring services will also be cancelled.

General

Any communication for us to you will be regarded as having been sent at the time shown on the communication or on our transmission logs. In any proceedings or dispute, our records certified as correct by the bank's employee in charge of the service channel, will be sufficient proof of any instructions you have provided or transaction you have performed on the service channels, the content or services on any service channel or value added service, unless you can prove otherwise. While we may give you extra time to comply with your obligations or decided not to exercise some of our rights, you must not assume that this means that our agreement with you has been changed or that it no longer applies to you. We can still insist on the strict application of any or all of our rights at a later stage. Every clause of the agreement and rules is severable from the others. If one or more of the clauses is invalid it will not mean the rest of the agreement or rules are invalid. The rest of the agreement and rules will still apply. Where dates and times need to be calculated the international standard time (GMT) plus 2 (two) hours will be used. This agreement will be governed by the laws of the Kingdom of Swaziland without giving effect to conflict of laws provisions.