



NEDBANK

**TERMS AND CONDITIONS
NEDBANK ID, TWO-FACTOR AUTHENTICATION MECHANISMS,
CLIENT-SIDE CERTIFICATES AND DIGITAL INTERACTION**

1 Introduction

- 1.1 **Digital interaction** means communication with and access to any services through any systems and devices.
- 1.2 **Systems and devices** mean any digital information systems, digital platforms, equipment, software, mobile devices and/or any other hardware devices.
- 1.3 When interacting digitally with Nedbank Group Limited or any of its subsidiaries (**Nedbank/we/us/our**), you will be required to use authentication mechanisms that allow you to access our services and products. An individual will be required to use one level, and a juristic entity two levels, of authentication. The authentication mechanisms are the following:
- **First level of authentication mechanism** (for individuals and juristic entities). The first level of authentication is the **Nedbank ID**, which consists of your username and password.
 - **Two-factor authentication (2FA) mechanism** (for juristic entities only). The second level of authentication is provided by Fast Identity Online (FIDO) hardware tokens and/or the Nedbank Business Authenticator app, which can be downloaded for free. Linked to the 2FA mechanism is the client-side certificate. The certificate complements the 2FA mechanism to protect you and us against the interception of communications. (Collectively '**authentication mechanisms**').

2 Binding terms

- 2.1 Please familiarise yourself especially with the **bold** text set out in the terms and conditions as it may:
- limit our or a third party's risk or liability;
 - create risk or liability for you;
 - compel you to indemnify us or a third party; and/or
 - mean that you acknowledge a fact.
- 2.2 Nothing in these terms and conditions is intended or must be understood to restrict, limit or avoid any rights or obligations you have in terms of the Consumer Protection Act, 68 of 2008, unlawfully.
- 2.3 These terms and conditions are in addition to the terms and conditions relating to your Nedbank account(s) or any other Nedbank service channels or products used by you.
- 2.4 If there is a dispute about any of the items listed in clause 2.6, these terms and conditions will apply. If there is a dispute about your Nedbank account, other service channels or products, the terms and conditions applicable to those will apply.
- 2.5 These terms and conditions are governed by the laws of the Republic of South Africa and will become binding on your acceptance of them.
- 2.6 These terms and conditions apply to:
- 2.6.1 your digital interaction with us;
 - 2.6.2 the creation of a Nedbank ID;
 - 2.6.3 the use of the 2FA mechanisms; and
 - 2.6.4 the client-side certificate.

3 Creating a Nedbank ID

- 3.1 To create a Nedbank ID, you will receive a prompt to enter your personal details on your device, which may include your identity number, name, surname, cellphone number and email address. If you are an existing Nedbank client, you may also use your existing profile, PIN and password to create a Nedbank ID.
- 3.2 You will then have to select a username and password, after which we will send you an Approve-it message to the cellphone number you gave us.
- 3.3 Once you have reacted positively to the message, your Nedbank ID will have been registered.
- 3.4 If you are using any of our services that require 2FA, you must enter your Nedbank ID details correctly to access such services.

4 Warranties

You warrant that you are duly authorised to:

- 4.1 **engage with us by way of digital interaction;**
- 4.2 create and register a Nedbank ID;
- 4.3 if applicable, apply for, accept and use a 2FA mechanism;
- 4.4 if applicable, select the Nedbank Business Authenticator app;
- 4.5 if applicable, act on behalf of the juristic entity that is or will become a user of our services;
- 4.6 if applicable, use your personal mobile device to access the Nedbank Authenticator app; and
- 4.7 accept these terms.

5 Freezing, suspension, modification, restriction and termination

- 5.1 We may freeze, suspend, modify or restrict your use of the authentication mechanisms or terminate your use of the authentication mechanisms immediately at any time without prior notice to you due to, including but not limited to, the following circumstances:
 - 5.1.1 Our being compelled to do so by law.
 - 5.1.2 Our having reasonable suspicion that the authentication mechanisms are being used for illegal, unlawful or fraudulent purposes.
 - 5.1.3 Your conduct resulting in a breach of our regulatory obligations.
- 5.2 We will give you reasonable prior notice if we want to freeze, suspend, modify or restrict your use of the authentication mechanisms or terminate your use of the authentication mechanisms due to, including but not limited to, the following circumstances, as determined at our sole discretion:
 - 5.2.1 Our being compelled to do so by law.
 - 5.2.2 Reputational risks or operational or business reasons.
 - 5.2.3 You no longer having a Nedbank account.
 - 5.2.4 You no longer qualifying for a Nedbank account according to our product specifications.
 - 5.2.5 You no longer qualifying for the authentication mechanisms.
 - 5.2.6 Your breaching these terms and conditions.
 - 5.2.7 Your breaching any other agreement with us.
 - 5.2.8 Your breaching any of the other service channel and/or product terms and conditions.
 - 5.2.9 Your doing anything (or allowing anything to be done) that we think may damage or affect the operation or security of the authentication mechanisms.

6 Privacy consent

- 6.1 You give us consent to process your personal information in relation to your applications for financial products and/or services with us, subject to our privacy policies and within the parameters of applicable laws. The processing will include, without limitation, conducting affordability assessments, credit scorings and any other profile building, that can help us appropriately allocate a product or service offering that is suited to your needs. The consent will also extend to us processing your personal information as we may deem fit for your and/or our legitimate interest.
- 6.2 You also give us the right to:
 - 6.2.1 collect your personal information from third parties when reasonably necessary and/or if it is impractical to collect the data directly from you;
 - 6.2.2 share your personal information with third parties if necessary, to provide financial products or services to you;
 - 6.2.3 process your personal information for purposes of complying with any legislative or regulatory requirements;
 - 6.2.4 transfer and/process your personal information outside the Republic of South Africa, where necessary, on condition that such transfer and/or processing is subject to applicable laws binding corporate rules or binding agreement; and
 - 6.2.5 process your special personal information (such as race, ethnic origin, biometric information or alleged criminal behaviour), only where necessary and subject to our privacy policies and applicable laws.
- 6.3 You have the right to:
 - 6.3.1 request confirmation from us, free of charge, whether or not we hold your personal information;
 - 6.3.2 request the record or a description of your personal information held by us;
 - 6.3.3 request information about all third parties who have, or have had, access to your personal information;
 - 6.3.4 correct or delete your personal information;
 - 6.3.5 withdraw your consent at any time by providing notice to us;

- 6.3.6 object to your personal information to be held by us; and
- 6.3.7 lay a complaint at the Information Regulator regarding your personal information in terms of the Promotion of Access to Information Act, 2 of 2000.

7 Your responsibilities and obligations

- 7.1 **You acknowledge that we are not responsible for the suitability or maintenance of any systems and devices that you use in relation to Nedbank ID, 2FA mechanisms, our services or any digital interaction with us.**
- 7.2 **You must:**
 - 7.2.1 **ensure that the most recent and applicable security software is installed on all systems and devices, and that there are no destructive programmes, such as viruses, worms and spyware on the systems and devices;**
 - 7.2.2 **adhere to all our operating, maintenance and security requirements and procedures (including encryption standards);**
 - 7.2.3 **take all reasonable precautions to protect all systems and devices and always keep them free of malware, and likewise, we will take all reasonable precautions to protect you and our services from malware;**
 - 7.2.4 **not jailbreak, root or circumvent any standard security settings that have been installed on any systems and devices;**
 - 7.2.5 **make sure that all systems and devices can communicate with ours and meet our specifications for the installation and configuration of any services;**
 - 7.2.6 **maintain software licence arrangements, pay licence fees and get the telecommunications lines, hardware, software and consumable materials (and any updates or upgrades) necessary to access and use our services;**
 - 7.2.7 **ensure the integrity, safekeeping and confidentiality of all communication lines, data, confidential information and the authentication mechanisms you use; and**
 - 7.2.8 **not operate or use any systems and devices in a manner that may be prejudicial to us.**

8 Safekeeping of authentication mechanisms

- 8.1 You may link only one Nedbank ID to the Nedbank Business Authenticator app.
- 8.2 You may share the FIDO hardware tokens.
- 8.3 Except as provided in 8.2 above, your authentication mechanisms are for your exclusive use
- 8.4 You must therefore:
 - 8.4.1 keep your Nedbank ID details, as well as 2FA mechanisms and client-side certificate, private and safe and take all reasonable precautions to prevent unauthorised or fraudulent use of that and/or any damage to that; and
 - 8.4.2 not disclose or respond to any requests for any of your Nedbank ID details to anyone or record your Nedbank ID details in any way that may result in it becoming known to anyone. Do not record your Nedbank ID details anywhere in any form.)
- 8.5 **You must inform us immediately when you become aware of or reasonably suspect any unauthorised access to, or compromise and/or use or loss, of your authentication mechanisms. You must have appropriate measures in place to minimise any loss or harm that may result from unauthorised access, including changing your Nedbank ID details.**
- 8.6 Once your correct Nedbank ID details have been entered, your chosen 2FA mechanism will be activated and the client-side certificate installed, we will accept and process your instructions, irrespective of whether any of your details may have been entered fraudulently or without your authority.
- 8.7 If you wish to change your Nedbank ID details, you must go to a Nedbank branch or contact your relationship manager or banker for help.
- 8.8 If you no longer have access to your current 2FA mechanisms and wish to reapply, contact your client administrator or complete the token replacement form on the Nedbank Business Hub landing page.
- 8.9 You must remove the FIDO hardware token or other tokens from your device, lock your device and close your applications while you are not transacting. Make sure that your tokens are always kept in a safe place.
- 8.10 **We will not be liable to you for any claims or losses incurred due to an unauthorised person gaining access to any one of your 2FA mechanisms or any of our services or because we acted on an instruction received from such unauthorised person.**

9 Digital interaction risks

You accept all risks attached to digital interaction with us. These risks include that:

- 9.1 **it may not be the safest way of instructing us as digital interaction may be tampered with before, during or after transmission and can be fraudulently manipulated;**
- 9.2 **receipt or execution of digital interaction may be delayed because systems and devices failed, malfunctioned or were unavailable;**
- 9.3 **digital interaction may be illegible or inaudible, which may lead to instructions not being executed as intended;**
- 9.4 **we cannot verify email addresses, fax numbers and signatures;**
- 9.5 **we cannot establish the identity or designation of the sender of the digital interaction;**
- 9.6 **we may not always be able to confirm receipt of digital interaction instructions; and**
- 9.7 **natural phenomena, riots, acts of vandalism, sabotage, terrorism, electricity interruptions or any other event beyond our control may affect the receipt or execution of communication through digital interaction.**

10 Liability

- 10.1 **Except where damage or loss arises directly or indirectly from our wilful misconduct or gross negligence (or any person acting for or controlled by us), we will not be liable to you for any damage or loss that you may suffer because of:**
 - 10.1.1 **any digital interaction;**
 - 10.1.2 **any access to your Nedbank ID details, the 2FA mechanism selected and used by you, the client-side certificate or from any breach of security or any destruction of your information;**
 - 10.1.3 **any action taken in terms of clause 5;**
 - 10.1.4 **any person having gained unauthorised access to any information or data;**
 - 10.1.5 **incorrect information having been given to us or to any person, and reliance thereon;**
 - 10.1.6 **the use of or inability to use your 2FA mechanisms, the client-side certificate and/or our services;**
 - 10.1.7 **any breach of these terms;**
 - 10.1.8 **an infringement of any intellectual property rights;**
 - 10.1.9 **any instruction you gave us, including any incorrect, illegible, incomplete or inaccurate information or data;**
 - 10.1.10 **any inadvertent delays in accessing or using our services;**
 - 10.1.11 **any use, misuse, abuse or possession of any software used to access our services;**
 - 10.1.12 **any unauthorised or unlawful access to any of your accounts or data or any loss, destruction or theft of or damage to any of your or our data or equipment;**
 - 10.1.13 **your failure to comply with any of your obligations or any banking and security procedures and requirements we have specified;**
 - 10.1.14 **any malfunction, distortion, interruption, failure, glitch, bug or defect experienced with, or the unavailability of, any systems and devices or communication links used in relation to our services;**
 - 10.1.15 **any security breaches caused by you or a third party;**
 - 10.1.16 **the destruction of or damage to our or your systems and devices because of power failures or similar occurrences;**
 - 10.1.17 **any false, fraudulent or altered instruction, mandate, consent, commitment or the like that is allegedly given by you;**
 - 10.1.18 **any lack of or failing in your authority to represent or act on behalf of any third party; and**
 - 10.1.19 **your acting outside of your mandate.**
- 10.2 **Any demand, claim or action arising against us in connection with the circumstances in this clause will be limited to direct damages. Special or consequential damages are hereby specifically excluded.**

11 Intellectual property rights

- 11.1 **We will retain all intellectual property rights to any of our authentication mechanisms, services, systems and devices, and documentation used to provide the services.**
- 11.2 **You may not duplicate, reproduce, decompile, reverse-engineer, create derivative works from or in any way tamper with any of our intellectual property or any device, certificate, software or documentation.**
- 11.3 **You may not infringe or misappropriate any of our or a third party's intellectual property or other proprietary rights when accessing and using our services and performing your obligations as recorded in these terms.**

12 Contact us

If you have any questions or want to report fraud or submit a complaint or claim in connection with your authentication mechanisms, call us on any of the numbers listed below.

Retail:	0860 555 111
Retail Relationship Banking:	0860 116 400
Retail Business Banking:	0860 111 055
Nedbank Corporate Invest Banking Service Desk:	010 217 4340

13 Alternative dispute resolution

- 13.1 We have a complaint process that is available through the Nedbank Contact Centre, any Nedbank branch, or at www.nedbank.co.za.
- 13.2 If you have a dispute or a complaint regarding our services, you will need to send us a written statement setting out the dispute or the complaint. We undertake to investigate your dispute or complaint within a reasonable time, keep you informed during the investigation and provide you with a final written response.
- 13.3 Should you not be satisfied with the response referred to above, you have the right to contact the Ombud for Banking Services and/or the Financial Sector Conduct Authority and/or the National Consumer Tribunal using the details below:

Ombud for Banking Services	Financial Sector Conduct Authority	National Consumer Tribunal
Tel: +27 (0)860 800 900 +27 (0)11 712 1800 Email: info@obssa.co.za Physical address: Ground Floor, 34 Fricker Road, Illovo, Johannesburg	Tel: 012 428 8000 012 428 8012 080 020 2087 080 011 0443 Fax: 012 347 0221 Email: info@fsca.co.za Physical address: Block B, Riverwalk Office Park, 41 Matroosberg Road, Ashlea Gardens, Pretoria, 0081 Postal address: PO Box 35655, Menlo Park, 0102	Tel: 010 006 0484 Fax: +27 (0)12 663 5693 Email: registry@nct.org.za Physical address: Ground Floor, Block B, Lakefield Office Park, 272 West Avenue, corner West Avenue and Lenchen Avenue North, Centurion