AGREEMENT FOR THE PROTECTION OF PERSONAL INFORMATION

Full name of the Supplier	together with its successors-in-title and all subsidiaries, affiliates and assigns (hereinafter referred to as the "**Supplier**")
Registration Number	
Physical Address	
Postal Address	
E-mail Address	

For and on behalf of the Supplier: (Who warrants that he/she is duly authorised)	
Date	
Place	
Signature	
Name	
Designation	

For and on behalf of Nedbank Limited Registration Number 1951/000009/06 ("Nedbank") (Who warrant that they are duly authorised)		
	First signatory	Second signatory
Date		
Place		
Signature		
Name		
Designation		

THE PARTIES AGREE AS FOLLOWS:

In the case of any Contract or ongoing relationship between the Parties, and where the provisions of POPI apply to the Processing of Personal Information in relation to the Services, these terms and conditions shall apply to and supplement the terms and conditions of such Contract.

In the event of a conflict between the provisions of this Agreement and the / a Contract, the provisions of this Agreement will take precedence in regard to all aspects pertaining to any Processing of Personal Information by the Supplier of any Data Subjects for Nedbank.

1. **DEFINITIONS AND INTERPRETATION**

1.1. "**Agreement**" means this Protection of Personal Information agreement;

1.2. "**Affiliate**" means with respect to a Party any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, including but not limited to Subsidiaries and associates that directly or indirectly, Control, are Controlled by, or are under common Control with a Party. For purposes of this Agreement, the term "Subsidiaries" shall have the meaning ascribed thereto in the South African Companies Act 71 of 2008, as amended;

1.3. "**Business Day**" means any day from Monday to Friday and excludes any public holiday as gazetted in the Republic of South Africa;

1.4. "**Confidential Information**" means any information or data of any nature, tangible or intangible, oral or in writing and in any format or medium, which (i) by its nature or content is, or ought reasonably to be identifiable as, confidential and/or proprietary to Nedbank or a third party associated to Nedbank, or (ii) is provided or disclosed in confidence, and which Nedbank or any person acting on behalf of Nedbank may disclose to the Supplier, or (iii) may come to the knowledge of the Supplier by whatsoever means. Without limitation, Confidential Information shall include the following –

1.4.1. information relating to Nedbank's business activities, business relationships, products, services, processes, data, and Staff, including agreements to which Nedbank is a party (including this Agreement);

1.4.2. information contained in or constituting or relating to Nedbank's technology and telecommunications systems including third party hardware and software, and associated material, and information or incidents concerning faults or defects therein;

1.4.3. Nedbank's technical, scientific, commercial, financial and market information, methodologies, formulae and trade secret;

1.4.4. Nedbank's architectural information, demonstrations, plans, designs, drawings, processes, process maps, functional and technical requirements and specifications and the data relating thereto;

1.4.5. Intellectual property that is proprietary to Nedbank or that is proprietary to a third party;

1.4.6. information relating to Nedbank's current and existing strategic objectives, strategy documents and plans for both its existing and future information technology, processing, business processing and business process outsourcing; and

1.4.7. Personal Information as defined in this Agreement.

1.5. "**Contract**" means any agreement and any annexures thereto, entered into between the Parties in respect the provision of Services by the Supplier to Nedbank;

1.6. "**Control**" means the ability, by virtue of ownership, right of appointment, voting rights, management agreement, or agreement of any kind, to control or direct, directly or indirectly, the board or executive body or decision-making process or management of such entity;

1.7. "**Data Subject**" means any person to whom the specific Personal Information relates, as contemplated in POPI;

1.8. "**Information Privacy Officer**" means Nedbank's Information Officer, as referred to in the Nedbank Group Access to Information Manual (as may be amended from time to time), compiled in terms of Section 51 of the Promotion of Access to Information Act 2 of 2000;

1.9. "**Operator**" has the meaning set out in POPI and for purposes of this Agreement means the Supplier and any authorised subcontractor of the Supplier;

1.10. "**Party**" or "**Parties**" means either the Supplier or Nedbank or both, as the context may require;

1.11. "**Personal Information**" has the meaning set out in section 1 of POPI, and includes special personal information as defined in section 26 of POPI and relates only to the Personal Information of which Nedbank is the Responsible Party and in relation to which the Supplier renders the Services;

1.12. "**POPI**" means the Protection of Personal Information Act No. 4 of 2013, as amended from time to time;

1.13. "**Processing**" or "**Process**" has the meaning set out in POPI;

1.14. "**Responsible Party**" has the meaning ascribed thereto in POPI, and for purposes of this Agreement shall mean Nedbank;

1.15. **"Services"** means any supply or rendering of services by the Supplier for Nedbank in terms of a Contract and in terms of which the Supplier *inter alia* Processes Personal Information of Data Subjects;

1.16. **"Signature Date"** means the date of signature of this Agreement by the last Party to do so in time;

1.17. "**Staff**" means any employee, independent contractor, agent, consultant, sub-contractor or other representative of either Party;

1.18. In this Agreement -

1.18.1. Words importing:

1.18.1.1. any one gender includes the other gender;

1.18.1.2. the singular includes the plural, and vice versa;

1.18.1.3. natural persons include created entities (corporate or unincorporated) and vice versa.

1.19. Any Party shall, where relevant, be deemed to be references to, or to include, as appropriate, their respective successors or permitted assigns.

1.20. References to statutory provisions shall be construed as references to those provisions as respectively amended, consolidated, extended or re-enacted from time to time and shall be construed as including references to the corresponding provisions of any earlier legislation directly or indirectly amended, consolidated, extended or replaced by those statutory provisions or re-enacted and shall include any orders, ordinance, regulations, instruments or other subordinate legislation made under the relevant statute.

2. **COMMENCEMENT AND DURATION**

This Agreement shall commence on the Signature Date hereof and shall continue to be of force and effect for as long as the Supplier remains in possession of any Personal Information of the Data Subjects, regardless of the termination of the Contract.

3. **PROTECTION OF PERSONAL INFORMATION**

3.1. It is recorded that, pursuant to its obligations under this Agreement, the Supplier will Process Personal Information of Data Subjects in connection with and for the purposes of the provision of the Services and will act as Nedbank's Operator for purposes of POPI.

3.2. Unless required by law, the Supplier shall Process the Personal Information only:

3.2.1. in compliance with this Agreement;

3.2.2. for the purposes connected with the provision of the Services or as specifically otherwise instructed or authorised by Nedbank in writing; and

3.2.3. in accordance with Nedbank's technical and organisational security measures as set out in Annexure A attached hereto, or agreed to by the Parties.

3.3. The Supplier shall treat the Personal Information that comes to its knowledge or into its possession as confidential and shall not disclose it without the prior written consent of Nedbank, unless required to do so by law. For avoidance of doubt, the provisions of the Contract in relation to Confidential Information or any non-disclosure agreement, or the provisions regarding confidentiality contained in any Contract, as the case may be, entered into between the Parties shall with the necessary changes, apply to this Agreement.

3.4. Without limiting the Supplier's obligations under this Agreement, the Supplier shall comply with applicable industry or professional rules and regulations, in relation to the safeguarding of Personal Information, which may apply to it.

3.5. Within 5 (five) Business Days of a request from Nedbank, the Supplier shall provide to Nedbank a written explanation and full details of the technical and organisational measures taken by or on behalf of the Supplier to demonstrate and ensure compliance with clause 3.2.3.In addition to any other obligations set out in clause 3, the Supplier shall:

3.5.1. take steps to keep abreast and ensure that it and its Staff comply fully with all applicable laws and regulations that are applicable to the Services;

3.5.2. limit the Processing of and access to the Personal Information to those Staff who need to know the Personal Information to enable the Supplier to render the Services;

3.5.3. deal promptly, but at all times without exceeding 5 (five) business days, with all reasonable inquiries from Nedbank relating to its Processing of the Personal Information and provide Nedbank with copies of the Personal Information in the format reasonably specified by Nedbank;

3.5.4. immediately inform Nedbank of its inability to comply with Nedbank's instructions and this clause 3, in which case Nedbank is entitled to suspend the Supplier's Processing of Personal Information and/or terminate the Contract and enforce clause 6 of this Contract subject to any legal retention requirements;

3.5.5. provide Nedbank with full co-operation and assistance in relation to any requests for access to, correction of or complaints made by the Data Subjects relating to their Personal Information;

3.6. The Supplier shall notify Nedbank in writing:

3.6.1. by sending an email to Nedbank's Information Officer or Nedbank Relationship Manager, to privacy@nedbank.co.za (as referred to in the Nedbank Group PAIA (Promotion to Access of Information) Manual as posted on Nedbank's website) within no later than 1 (one) Business Day, but preferably immediately, of becoming aware or suspecting any unauthorised or unlawful use, disclosure or Processing of Personal Information or if any Personal Information under the control of the Supplier as a result of this Agreement has been or may reasonably believe to have been accessed or acquired by an unauthorised person or if a breach has occurred with reference to the Supplier's use of the Personal Information under this Agreement, and

3.6.2. furnish Nedbank with details of the Data Subjects affected by the compromise and the nature and extent of the compromise, including details of the identity of the unauthorised person who may have accessed or acquired the Personal Information as well as with daily reports on progress made at resolving the compromise;

3.6.3. within 3 (three) Business Days of receipt thereof, of any request for access to or correction of the Personal Information or complaints received by the Supplier relating to Nedbank's obligations in terms of POPI and provide Nedbank with full details of such request or complaint; and

3.6.4. promptly of any legally binding request for disclosure of Personal Information or any other notice or communication that relates to the Processing of the Personal Information from any supervisory or governmental body.

3.7. The Supplier acknowledges and agrees that Nedbank retains all right, title and interest in and to the Personal Information and that the Personal Information shall constitute Nedbank's Confidential Information.

4. **AUDIT RIGHTS**

Nedbank or its agent shall have the right to audit the Supplier at any time, with reasonable notice, if there is a reasonable, suspicion that the Supplier is not complying with the provisions of this Agreement or where there is a suspicion that the confidentiality, integrity and accessibility of Personal Information is likely to be compromised. Such audit rights shall include but not be limited to the right of access to systems, procedures and software, and inspection of the physical security of the Supplier's premises. The Supplier shall offer reasonable assistance and co-operation to Nedbank and/or its auditors or inspectors in the carrying out of such auditing exercise. To the extent that the Supplier engages an independent auditor in relation to the provisions of applicable personal data protection legislation to

carry out an audit of its operations, the Supplier agrees to provide Nedbank with copies of the audit reports of all such audit exercises. Nothing in this clause 4 should be read as providing Nedbank with unlimited access to audit the Supplier without just cause.

5. **SEPARATION OF PERSONAL INFORMATION**

The Supplier shall Process the Personal Information in relation to the Services separately from Personal Information, data and property relating to the Supplier or any third party, and may not be combined or merged with information of another party unless otherwise agreed to in writing by Nedbank.

6. **RETURN AND RETENTION OF PERSONAL INFORMATION**

6.1. Nedbank may, at any time on written request to the Supplier, require that the Supplier immediately return to it any Personal Information and may, in addition, require that the Supplier furnish a written statement to the effect that upon such return, it has not retained in its possession or under its control, whether directly or indirectly, any such Personal Information or material.

6.2. Alternatively, the Supplier shall, as and when required by Nedbank on written request, destroy all such Personal Information and material and furnish Nedbank with a certificate of destruction to the effect that the same has been destroyed, unless the law prohibits the Supplier from doing so. In that case, the Supplier agrees that it will maintain the confidentiality of the Personal Information taking into account clause 2 and will not actively Process the Personal Information any further.

6.3. The Supplier shall comply with any request in terms of this clause 6 within 7 (seven) days of receipt of such request.

7. **SUBCONTRACTING**

7.1. The Supplier may not subcontract the performance of any of its obligations under this Agreement without Nedbank's prior written consent having been obtained. All references to the Supplier's Staff shall be deemed to include the employees of any sub-contractor of the Supplier.

7.2. In the event that Nedbank agrees to the Supplier sub-contracting certain or all of the Supplier's obligations, the Supplier must only do so by way of a written contract with the sub-contractor which contract must impose the same obligations on the sub-contractor as are imposed on the Supplier in terms of this Agreement insofar as the Processing of Personal Information by the sub-contractor is concerned.

8. **INDEMNITIES**

Subject to the Contract, the Supplier hereby indemnifies and holds harmless Nedbank from any and all losses arising from any claim or action brought against Nedbank arising from or due to the Supplier's breach of its obligations set out in this Agreement or any law with respect to the protection of Personal Information and Confidential Information.

9. **CONFIDENTIALITY**

9.1. The Supplier agrees and undertakes –

9.1.1. Except as permitted by this Agreement, not to disclose or publish any Confidential Information in any manner for any reason or purpose whatsoever without the prior written consent of Nedbank and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Supplier to obtain the consent of such third party;

9.1.2. Except as permitted by this Agreement, not to utilise, employ, exploit or in any other manner whatsoever use the Confidential Information for any purpose whatsoever without the prior written consent of Nedbank and provided that in the event of the Confidential Information being proprietary to a third party, it shall also be incumbent on the Supplier to obtain the consent of such third party;

9.1.3. To restrict the dissemination of the Confidential Information to only those of its Staff who are actively involved in activities for which use of Confidential Information is authorised and then only on a "need to know" basis and the Supplier shall initiate, maintain and monitor internal security procedures reasonably acceptable to Nedbank to prevent unauthorised disclosure by its Staff; and

9.1.4. To take all practical steps, both before and after disclosure, to impress upon its Staff who are given access to Confidential Information the secret and confidential nature thereof.

9.2. The obligations of the Supplier with respect to each item of Confidential Information shall endure for an indefinite period from receipt of that item of Confidential Information. The obligations referred to in this clause 9 shall endure notwithstanding any termination of this Agreement, any other agreement entered into between the Parties or any discussions between the Parties.

9.3. The Supplier hereby indemnifies and holds Nedbank harmless from any and all losses arising from, or in connection with, any claim or action arising from the Supplier's breach of any obligation with respect to Confidential Information.

10. **NEDBANK AFFILIATE**

Unless otherwise agreed to the contrary, the Parties hereby agree that any Nedbank Affiliate shall be entitled to rely on all the provisions of this Agreement, which provisions are binding between the Nedbank Affiliate and the Supplier, in respect of any contract that might be entered into between the Supplier and the Nedbank Affiliate in terms of which the Supplier will be Processing Personal Information on behalf of the Nedbank Affiliate. For the avoidance of doubt, this Agreement is applicable and binding in respect of all contracts concluded between the Supplier and Nedbank or Nedbank Affiliate where the Supplier Processes Personal Information on behalf of Nedbank or the Nedbank Affiliate.

11. **BREACH AND TERMINATION**

11.1. In the event of either of the Parties committing a breach of any of the conditions of this Agreement and failing to remedy such breach within 7 (seven) Business Days of receipt of a notice from the other Party requesting it to remedy such breach, then the other Party shall be entitled to cancel this entire Agreement forthwith and claim such losses as it may have suffered. In the event of termination of this Agreement, the Party terminating this Agreement shall have a right to also exercise its rights of termination under the Contract.

11.2. Notwithstanding anything to the contrary contained in this Agreement, the Parties shall be entitled to terminate this Agreement by mutual agreement in writing.

11.3. The provisions of this clause 11 shall not affect or prejudice any other rights/remedies which the Parties may have in law or in any other Contract between the Parties.

12. **CONSEQUENCES OF TERMINATION**

12.1. The termination of this Agreement shall not affect the rights of either of the Parties that accrued before termination of this Agreement or which specifically survives the termination of the Agreement.

12.2. Upon termination of this Agreement or upon request by Nedbank, the Supplier shall return or destroy any material containing, pertaining or relating to the Personal Information disclosed pursuant to this Agreement to Nedbank in terms of clause 6 unless the law prohibits the Supplier from doing so. In that case, the Supplier agrees that it will maintain the confidentiality of the Personal Information and will not, under any circumstance, Process the Personal Information any further.

13. **WAIVER**

13.1. Failure or delay by either Party in exercising any right will not constitute a waiver of that right.

13.2. No waiver of any of right under this Agreement will be binding unless it is in writing and signed by the Party waiving the right.

14. **SEVERABILITY**

If any part of this Agreement is found to be invalid or unenforceable, it shall be severed from the remainder of this Agreement, which shall remain valid and enforceable.

15. **CESSION AND DELEGATION**

The Supplier may not cede its rights or delegate its obligations in terms of this Agreement, without the prior written consent of Nedbank, which consent shall not be unreasonably withheld.

16. **GOVERNING LAW**

This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed exclusively in accordance with South African law. The Supplier consents and submits to the jurisdiction of the South Gauteng High Court in any dispute arising from or in connection with this Agreement. Without prejudice to any other rights or remedies which Nedbank may have, the Supplier acknowledges that nothing herein shall preclude Nedbank from seeking urgent relief or specific performance from a court of competent jurisdiction.

17. **NOTICES AND DOMICILIUM**

17.1. The Supplier selects as its *domicilium citandi et executandi* the physical address appearing on the first page, and for the purposes of giving or sending any notice provided for or required hereunder, the address and telefax number appearing on the first page or such other addresses or email address as may be substituted by notice given as herein required.

17.2. The Supplier acknowledges that any notice it sends to Nedbank relating to this Agreement shall be marked for the attention of Nedbank's **Information Privacy Officer** ("**IPO**").

17.3. Nedbank selects as its *domicilium citandi et executandi* 135 Rivonia Road, Sandown, Sandton, 2196 and for the purpose of giving or sending any notice provided for or required hereunder, or such other addresses or email as may be substituted by notice given as herein required.

17.4. Any notice addressed to a Party at its physical or postal address shall be sent by prepaid registered post, or delivered by hand, or sent by email.

17.5. Any notice shall be deemed to have been given and received –

17.5.1. if posted by prepaid registered post, 7 (seven) days after the date of posting thereof;

17.5.2. if hand delivered, on the day of delivery; and

17.5.3. if sent by email on the date of sending of such email, unless the contrary is proven, provided that such notice shall be confirmed by prepaid registered post on the date of despatch of such email or, should no postal facilities be available on that date, on the next business day.

17.6. Notwithstanding anything to the contrary contained in this clause 17 a written notice or communication actually received by a Party shall constitute adequate written notice or communication to it notwithstanding that it was not sent or delivered to its chosen *domicilium citandi et executandi* or in the manner provided in this clause 17.

ANNEXURE A

Technical and organisational security measures

1. **Definitions:**

1.1. "**Board**" means Supplier's board of directors or that of its affiliated entities, and/or its authorised subcontractors;

1.2. "**Cyber security**" or "**Information Security**" means protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide; and

1.3. **"Supplier**" means any organisation that has entered into a contract (formally, verbally or through conduct) with Nedbank Limited or any of Nedbank Limited affiliated entities, either in its right as a main contractor and/or as subcontractor or any of its affiliated entities doing business with Nedbank.

2. **THE SUPPLIER WILL ENSURE THAT THE FOLLOWING SECURITY MEASURES ARE IMPLEMENTED AND ADHERED TO**

2.1. Security Governance Framework

2.1.1. A framework for cyber security governance is established;

2.1.2. There is a clear commitment demonstrated by the Board and/or Supplier's senior management to ensure that Supplier's overall approach to cyber security supports high standards of corporate governance.

2.2. Security Direction

2.2.1. The Board and/or Supplier's senior management shall provide cyber security direction through its governance structures

2.3. Cyber Security Strategy

2.3.1. A cyber security strategy must be formulated and maintained in line with the Suppliers strategic objectives.

2.4. Cyber Security Assurance

2.4.1. The Supplier shall adopt a consistent and structured approach for cyber security risk management using structured methodologies

2.4.2. The Supplier may also be asked to provide assurance reports to Nedbank or Nedbank may request to conduct certain assurance assessments.

2.5. Business Impact Assessment

2.5.1. The Supplier shall identify its most critical assets (crown jewels) in relation to the services provided to Nedbank and perform risk assessment on such assets that will guide the Supplier to implement the necessary controls to protect against compromise of confidentiality, integrity and availability of information and systems.

2.5.2. Nedbank may request a view of these business impact assessments or attestations that these have been conducted and any gaps remediated.

2.6. Threat Profiling

2.6.1. Threats and related threat events to key information systems must be identified, profiled, prioritised and recorded to determine and assess the likelihood of the threat event occurring.

2.7. Vulnerability Assessment

2.7.1. A process must be established to identify and assess the vulnerabilities and relevant controls in the environment to be assessed (e.g. penetration testing, red team testing).

2.7.2. Continuous vulnerability scanning must be utilised to identify security and patch deficiencies.

2.8. Cyber Security Policies, Standards and Procedures

2.8.1. Comprehensive, documented cyber security policies, standards and procedures must be in place and communicated to all staff, including contractors and temporary workers, where applicable.

2.8.2. An acceptable use policy (AUP) must be established, which defines how your employees and contractors can use Nedbank data and systems, including software, computer equipment and connectivity.

2.9. Cyber Security Function

2.9.1. A cyber security governance structure including a specialist cyber security function must exist, which has responsibility for promoting cyber security to ensure good practice in cyber security is applied effectively and consistently throughout the Suppliers organisational structures.

2.9.2. Roles and responsibilities for cyber security must be assigned in terms of an agreed RACI chart.

2.9.3. The cyber security function must perform sufficient collections, monitoring, investigation and remediation of cyber security related events to detect, investigate and respond to potential or actual cyber security incidents in an effective manner.

2.10. Projects

2.10.1. New projects that impact on any of the services that are provided to Nedbank must align with the organisation's project management process, consider cyber security requirements and be run in a systematic and structured manner.

2.11. Legal and Regulatory Compliance

2.11.1. A process must be established to identify and interpret the cyber and privacy related security implications of relevant laws and regulations to ensure compliance.

2.12. Employment Life Cycle

2.12.1. Cyber security requirements must be embedded into each stage of the employment life cycle, specifying security related actions required during the induction of each employee, their ongoing management and termination of their employment.

2.13. Remote Working

2.13.1. Staff working in remote environments that will process Nedbank data or provide services to Nedbank (e.g. in locations other than the organisation's premises) must be subject to identification, authentication and authorisation compliant with FIPS 140, must protect computing devices and the information they handle against loss, theft and cyber-attack; be supported by security awareness material and employ additional security controls and vigilance when travelling.

2.14. Security Awareness Programme

2.14.1. A security awareness programme must be implemented, to promote security awareness to all individuals who have access to the Supplier's information and systems, to create a culture where expected security behaviour is embedded into regular day-to-day activities of all relevant individuals.

2.15. Mobile Device Protection

2.15.1. Mobile devices used to provide any services to Nedbank or that process Nedbank confidential information must be configured to be secure in order to prevent a potential security compromise of the data on the device and provided with secure means of connecting to the network.

2.16. Consumer Devices (BYOD)

2.16.1. Personal mobile devices used for fulfilment of any services provided to Nedbank (BYOD) must be supported by documented agreements with staff, and technical security controls implemented to protect business information to ensure critical and sensitive business information handled on BYOD devices receives the same level of protection as that provided by corporate-owned equipment.

2.16.2. BYOD solutions must incorporate secure encapsulation (secure container) of scoped Nedbank data stored on BYOD devices.

2.17. System Development Methodology

2.17.1. Development activities must be carried out in accordance with a documented system development methodology to ensure that business applications (including those under development) meet business and cyber security requirements.

2.17.2. System development activities must be performed in specialised development environments, which are isolated from the live and testing environments, and protected against unauthorised access to provide a secure environment for system development activities and avoid any disruption to business activity.

2.17.3. Development of End User Developed Applications (EUDA) must be carried out in accordance with a documented development methodology to ensure EUDA meet security requirements.

2.18. Data destruction

2.18.1. Where electronic media and data is destroyed, this must be done securely using the NIST800-88 wiping standard

2.18.2. Physical documents and data on permanent medium must be destroyed with a category 4 shredder and if a shredder cannot be used, in a manner that will not allow recovery of the data e.g. incineration.

2.18.3. A certificate of destruction must be issued to Nedbank validating the NIST process was used.

2.19. Application Protection

2.19.1. Business applications must be protected by using sound security architecture principles ie TOGAF.

2.20. Web Application Protection

2.20.1. Specialised procedural and technical controls such as a Web Application Firewall must be applied to all Internet-facing web applications, web content and websites, that may provision access to Nedbank data.

2.21. Information Validation

2.21.1. Business applications must incorporate security controls that protect the confidentiality and integrity of information when it is input into, processed by and output from these applications.

2.22. Access Control

2.22.1. Access control methods must be established to restrict access to business applications, systems, networks, computing devices and physical information that will be used to provide services to Nedbank, by all users and devices, who must be assigned specific privileges based on what the user needs to know or access, to enable them to perform their duties but do not permit them to exceed their authority.

2.22.2. Access control mechanisms (eg passwords, tokens, biometric or any combination of these) must be used to identify, authenticate and authorise users before being granted access to business applications, systems, networks, computing devices and physical information.

2.23. User Authorisation

2.23.1. All individuals with access to business applications, systems, networks, computing devices and physical information must be authorised before they are granted access privileges based on what the user needs to know or access.

2.23.2. By default, users will not be authorised to perform any activity on business applications, systems, networks, computing devices and physical information unless explicitly authorised.

2.23.3. Activities that could provide extensive privileges and misuse if combined, must be segregated between users.

2.24. Computer and Network Installations

2.24.1. Computer system, network and telecommunication installations, including data centres must be designed to incorporate the required security controls to meet the security requirements of the critical business applications they support.

2.25. Data Encryption

2.25.1. All data at rest must be encrypted and where possible, with a unique Key only used for Nedbank data. Data must be encrypted with AES 256-bit key length (Advanced Encryption Standard). Where possible the key must be Managed by Nedbank.

2.25.2. Data in motion must also be encrypted in both WAN and LAN environments with either TLS 1.2 or higher (Transport Layer Security), IPSec or equivalent standards.

2.26. Operating System and Database Configuration

2.26.1. Operating systems and databases must be configured to be secure in order to prevent a potential security compromise of the data on the devices as well as other computer installations or environments.

2.27. Virtualisation

2.27.1. Virtual instances must be subject to approval, deployed on robust, secure physical hardware and configured to segregate sensitive information to prevent business disruption as a result of system overload or disclosure of sensitive information to unauthorised individuals.

2.28. Network Storage Systems

2.28.1. Network storage systems must be protected using system and network controls to ensure they are available when required and do not compromise the security of information they store.

2.29. Back-up

2.29.1. All back-ups must be encrypted with AES 256-bit key length (Advanced Encryption Standard), to ensure the confidentiality and non-repudiation of the back-up information.

2.29.2. The organisation must be able to identify which back up media was used to back up any Nedbank data.

2.30. Change Management

2.30.1. Changes to business applications, computer systems and networks must be tested, reviewed and applied using a change management process to ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.

2.31. Network Design and Device Configuration

2.31.1. Network devices (including routers, switches, wireless access points and firewalls) must be configured according to documented configuration standards and configured to be secure in order to prevent a potential security compromise of the data on the network.

2.31.2. The network must be securely designed in order to prevent a potential security compromise of the data on the network.

2.32. Wireless Access

2.32.1. Wireless access must be authorised, users and computing devices authenticated, and wireless traffic encrypted to ensure that only authorised individuals and computing devices gain wireless access to networks and limit the risk of wireless transmissions being intercepted.

2.32.2. Wireless monitoring and intrusion prevention technologies must be employed.

2.32.3. Wireless networks must be compliant with latest NIST WiFi security guide.

2.33. External Network Connections

2.33.1. All external network connections to computer systems and networks must be individually identified, verified, recorded, and approved by the information systems or network owner.

2.34. Firewalls

2.34.1. Network traffic must be routed through a firewall, well configured according to documented standards, prior to being allowed access to networks, or before leaving networks.

2.35. Remote Maintenance

2.35.1. Remote maintenance of critical systems and networks must be restricted to authorised individuals, confined to individual sessions, and subject to review.

2.36. Collaboration Platforms

2.36.1. Collaborations platforms must be protected by setting management policies, deploying application controls, configuring the security settings of each platform and improving the security of supporting technical infrastructure to ensure that collaboration platforms are available when required, the confidentiality and integrity of information is protected in transit, and the risk of misuse is minimised.

2.37. Supplier's Third-Party Management Processes and Procedures

2.37.1. A security management framework must be established that includes appropriate external supplier security steering groups, policies, processes, registers and information risk assessments and security arrangements to ensure information risks are identified and managed effectively throughout all stages of the relationship with external suppliers.

2.37.2. A process must be established to integrate security into the procurement of products and services from external suppliers.

2.37.3. The use of products and services provided by external suppliers must be supported by contracts that include appropriate security requirements for products and services provided by external suppliers and specify how they will be met.

2.38. Cloud Security Management

2.38.1. A comprehensive, documented security management approach for the acquisition and use of cloud services must be developed and communicated to individuals who may purchase, develop, configure or use cloud services to ensure all necessary security arrangements are implemented for the use of cloud services, and ensure that information risks are managed.

2.38.2. A set of fundamental cloud security controls based on the security guidance by the Cloud Security Alliance must be created and implemented.

2.39. Patch Management

2.39.1. A process must be established for the deployment of system and software patches to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of vulnerabilities being exploited and serious business impact arising.

2.40. Malware Protection Software

2.40.1. Effective malware protection software must be installed, configured, and maintained to protect against malware attacks and ensure malware infections can be addressed within defined timescales.

2.41. Identity and Access Management

2.41.1. Identity and access management arrangements must be established to provide effective and consistent user administration, identification, authentication and access control mechanisms.

2.41.2. Accounts accessing Nedbank data must be approved by the Nedbank relationship manager.

2.41.3. Quarterly access reviews must be performed on all accounts accessing Nedbank systems and data.

2.42. Intrusion Detection / Prevention

2.42.1. Intrusion detection and prevention mechanisms must be applied to critical systems and networks to identify suspected or actual malicious attacks and enable the Supplier to respond before serious damage is done.

2.43. Information Leakage Protection

2.43.1. Information leakage protection mechanisms must be applied to systems and networks that process, store or transmit sensitive information to detect sensitive information that may be at risk of unauthorised disclosure.

2.44. Critical Infrastructure

2.44.1. Information systems that support or enable critical infrastructure must be protected by comprehensive security arrangements, which include security planning, cyber risk assessment and control selection, deployment, and monitoring

2.45. Cryptographic Solutions

2.45.1. Cryptographic solutions must be used to protect the confidentiality of sensitive information, preserve the integrity of critical information and confirm the identity of the originator of transactions or communications.

2.45.2. Cryptographic keys must be managed securely and protected against unauthorised access or destruction to ensure that they are not compromised, thereby exposing critical or sensitive information to attack.

2.45.3. Where technically feasible, cryptographic keys must be managed by Nedbank

2.46. Technical Vulnerability Management

2.46.1. A process must be established for the identification and remediation of technical vulnerabilities in business applications, systems, equipment and devices to address technical vulnerabilities quickly and effectively, reducing the likelihood of them being exploited, which could result in serious security incidents.

2.47. Security Event Logging and Monitoring

2.47.1. Important security-related events must be recorded in logs, stored centrally, protected against unauthorised change and analysed on a regular basis to help in the identification of threats that may lead to a cyber security incident, maintain the integrity of important security related information and support forensic investigations.

2.47.2. Security-related data must be reviewed and analysed on a regular basis, by security specialists, using a combination of automated and manual methods to identify anomalous activity or behaviour, triage accordingly and report and report security incidents requiring response in a timely manner.

2.48. Threat Intelligence

2.48.1. Threat intelligence must be created, based on analysis of a range of sources, which is relevant, insightful, contextual and actionable to provide situational awareness about current and emerging threats, supporting cyber risk-related decisions and activities.

2.49. Cyber Security Incident Management and Response

2.49.1. A cyber security incident management framework must be established, including relevant individuals, information and tools required by the Supplier's cyber security incident management process to provide the resources required to help resolve cyber security incidents quickly and effectively.

2.49.2. Nedbank must be informed of all cyber security incidents that involves Nedbank related systems or data immediately but no later than 24 hours of being detected and the Supplier will assist Nedbank with efforts to minimise the impact of such an incident.

2.49.3. Cyber security incidents must be identified, responded to, recovered from, and followed up using a cyber security incident management process to identify and resolve cyber security incidents quickly and effectively, minimise their business impact and reduce the risk of similar incidents occurring.

2.49.4. Arrangements must be made to protect the Supplier's information and systems against sophisticated, targeted cyber-attacks, supported by a Computer Security Incident Response Team (CSIRT) and Security Incident Response Plan (SIRP) to reduce the frequency and impact of attempted and successful targeted cyber-attacks.

2.49.5. A cyber security crisis management process must be established, supported by a Cyber Crisis Management Team (CCMT), which details actions to be taken in the event of a major cyber security incident, or serious attack to respond to major cyber security incidents and serious attacks quickly and effectively, reducing any potential business impact including brand and reputational damage.

2.49.6. Detailed response strategies and tactics (playbooks) for different cyber scenarios that could affect Nedbank must be created. The CCMT must be made up of specialist functions and management from the affected business or cluster.

2.50. Physical Protection

2.50.1. All critical facilities (including locations that house computer systems such as data centres, networks, telecommunication equipment, sensitive physical material and other critical assets) must be physically protected against accident or attack and unauthorised physical access.

2.50.2. All physical access to environments where Nedbank data is hosted must be recorded.

2.51. Cyber Security Testing

2.51.1. Critical systems and environments, including environments where Nedbank data resides, must be subject to security testing, using a diverse range of assessments (eg red team testing, penetration testing, vulnerability assessments and cyber security exercises) to identify security weaknesses in target environments and determine the level of resilience under attack conditions.

2.52. Cyber Security Compliance Monitoring

2.52.1. A security compliance management process must be established, which comprises cyber security controls derived from regulatory and legal drivers and contracts to help ensure cyber security controls are consistently prioritised and addressed according to cyber security obligations associated with legislation, regulations, industry standards or security requirements in contracts.

2.53. Nedbank Cyber and Privacy Risk Management Process

2.53.1. The Supplier will participate in the Nedbank Cyber and Privacy Risk Management process.

2.54. Assurance

2.54.1. The Supplier must be subject to an annual SOC2 Type II audit by an accredited assurance provider to obtain assurance that controls operated adequately and effectively over a period of time.

2.54.2. Any other agreed upon methodology must be approved by Nedbank Business Information Security Officer and Nedbank Cluster Risk Officer.

2.54.3. The scope of the audit must be in line with an industry recognised standard and framework as per Schedule A attached hereto.

2.54.4. Results must be shared with Nedbank in an expedient manner and uploaded to the Nedbank Archer system.

2.54.5. Nedbank may request from time to time supporting information for trouble shooting Nedbank related data and systems such as logs and the output of scripts and utilities.

3. **Schedule A**

3.1. The following list of standards and frameworks are acceptable for assurance purposes:

3.1.1. NIST Cybersecurity Framework

3.1.2. NIST 800-53 security standards

3.1.3. ISO27001/2 standards

3.1.4. CIS Benchmark standards

3.1.5. ISAE3402 / SSAE16