Level 1 Policy for Anti-money-laundering, the Combating of the Financing of Terrorist and Countering of Proliferation Financing and Related Activities and Sanctions

Ref: Trevor Adams, 2022

NEDBANK

1 Why we need this policy

Nedbank Group (the Group) will not be associated with money laundering (ML), terrorist financing (TF) or proliferation finance (PF) and has introduced policies, principles, methodologies, processes, systems and training to ensure that it meets its statutory duties and regulatory obligations or, if they do not exist, agreed standards.

Inadequate customer due diligence (CDD) and understanding of a client's background, nature and intended purpose for establishing a business relationship may expose the Group to undue ML, TF or PF risk. The Group must conduct enhanced due diligence (EDD) on clients who are likely to pose a higher risk to the Group.

In most jurisdictions it is a criminal offence to establish a business relationship or conclude a transaction in breach of financial sanctions legislation with individuals or entities that appear on sanctions lists or are involved in sanctioned activity or goods.

The Group must take reasonable measures to identify any business relationship, transaction or prospective business relationship or transaction involving individuals, entities, countries, goods or activities targeted in applicable financial sanctions legislation as much as possible and apply measures to combat the proliferation of weapons of mass destruction and other sanctioned activities.

The Group will take reasonable steps to ensure that finance or any other form of financial services it provides is not used to benefit sanctioned individuals or entities or to carry out sanctioned activity or any activity involving sanctioned goods or the proliferation of weapons of mass destruction.

The Group will take reasonable measures to identify and manage any business relationship or prospective business relationship or single transaction involving persons appearing on the Group's do- not-engage (DNE) list of the group.

2 Goal of this policy

This policy sets out the obligations of the Group relating to the following:

- Anti-money-laundering (AML).
- The combating of financing of terrorist and related activities (CFT).
- The countering of proliferation financing and related activities (CPF).
- Sanctions risk and internal-lists management.

The goals of this policy are the following:

- To support the Risk Management and Compliance Programme (RMCP), through which ML, TF, PF, sanctions risk and internal-list requirements are managed via risk-based principles, methodologies, processes, systems and training so that the Group can carry out and meet its statutory duties and regulatory obligations.
- To reduce reputational, operational, concentration, financial and legal risks to the Group, with the Group thereby meeting local and international standards.

This policy summarises the responsibility of management and employees for establishing a RMCP with regard to the following:

- Establishing an AML, CFT, CPF and sanctions strategy.
- Establishing a ML, TF, PF and sanctions risk appetite.
- Creating and implementing AML, CFT, CPF and sanctions risk- based principles, methodologies, processes, systems and training related to enterprise risk assessment, client risk assessments, CDD, ongoing due diligence (ODD), domestic prominent influential persons (DPIPs) and foreign prominent public officials (FPPOs).
- Declining or terminating business relationships or transactions due to ML, TF, PF, sanctions and internal-lists risks.
- Performing ML, TF, PF, sanctions and internal-lists reporting.
- Performing AML, CFT, CPF, sanctions and internal-lists recordkeeping.
- Conducting AML, CFT, CPF, sanctions and internal-lists training awareness and communication.
- Performing AML, CFT, CPF and sanctions governance and oversight, including ensuring clear and defined roles and responsibilities regarding AML, CFT, CPF and sanctions.
- Registering accountable and reporting institutions.
- Performing AML, CFT, CPF, sanctions and internal-lists monitoring.
- Performing AML, CFT, CPF, sanctions and internal-lists management reporting.
- Preventing, detecting, monitoring and reporting confirmed, suspected, detected or prevented ML, TF, PF, sanctions or internal-lists breaches.
- Identifying and managing any business relationship or prospective business relationship or single transactions involving individuals, entities, countries, goods or activities targeted in financial sanctions legislation.
- Identifying and managing any business relationship or prospective business relationship or single transaction involving persons listed on the internal lists of the Group.
- Identifying any vendors, suppliers and employees targeted in financial sanctions legislation.
- Conducting sanctions and internal-list screening.
- Conducting DNE list screening.
- Implementing principles in branches, subsidiaries, representative offices and other operations.

2.1 Review

This policy must be reviewed annually, and any material amendments are to be ratified by the board of directors.

2.2 Breach of policy

Employees in breach of this policy will be dealt with in terms of the Group disciplinary code and processes and may face criminal prosecution.

3 Where this policy applies

This policy:

- affects the Group;
- applies to employees, contractors, temporary employees, consultants, clients, shareholders, vendors and outside

agencies;
- applies to the majority-owned subsidiaries of the Group (If the Group does not majority-own or control a subsidiary, the Group must use its rights to ensure as far as practicable that the principles and standards contained in this policy are complied with;
- applies to representative offices; and
- must be read together with:
  - specific legislation for the jurisdiction in which a business unit, subsidiary or branch or representative office operates;
  - country-specific regulatory and supervisory rules, guidance notes, public compliance communications, directives and circulars, etc; and
  - the Nedbank Group RMCP.

4 Key principles

The key principles of this policy are detailed below.

4.1 Creation of policies, principles methodologies, processes, systems and training

The Group has introduced risk-based policies, principles, methodologies, processes, systems and training to ensure that it:
- meets regulatory requirements;
- meets agreed standards;
- manages and mitigates the risk of possible ML, TF, PF and sanctions breaches associated with business relationships and single transactions and cross-border transactions;
- manages and mitigates the risk of possible sanctions breaches; and
- manages and mitigates the risk associated with a person listed on an internal list or the DNE list.

Policies, principles, methodologies, processes, systems and training on risk-based AML, CFT, CPF, sanctions risk and internal- list management must be:
- developed;
- implemented;
- monitored; and
- continually reviewed and refined.

Establishment of a risk management and compliance programme

The Group has established a RMCP to manage risks associated with ML, TF, PF and sanctions.

4.2 Money laundering, terrorist-financing and sanctions risk strategy

The Group endeavours to proactively and reactively identify and assess ML, TF, PF and sanctions risks in order to identify possible risk mitigation and risk strategies to enhance its ML, TF, PF and sanctions risk management.

4.3 ML, TF, PF and sanctions risk appetite

The Group will not knowingly do or allow the following from happening:
- Facilitate ML, TF, PF and sanctioned activities.
- Establish or continue business relationships or conclude a single transaction with high-risk clients if the Group has not conducted EDD on them.
- Establish or continue business relationships or conclude a single transaction with clients that would expose the Group to reputational, operational or legal risks because of not complying with policies or any regulation associated with the policies.
- Have clients who insist on anonymity or give fictitious names.
- Have clients who are oral trusts of which have not been reduced to writing.
- Have clients who are Crypto asset Service Providers (CASPs)
- Have clients who are shell banks.

The Group recognises that a breach of AML, CFT, CPF and sanctions and risk appetite expressions could happen despite its best efforts. The Group will at all times have risk mitigating and remediation plans in place to limit the chances of breaches inadvertently happening.

4.5 Customer due diligence

When establishing a business relationship or concluding a Single Transaction with a client, the Group must apply appropriate CDD measures, taking into account the regulatory requirements for CDD, as well as ML, TF, PF and sanctions risk assessments.

Obtaining this information will facilitate the upfront risk profiling of clients and ithe identification of suspicious or unusual activities and transactions.

The Group must conduct ODD as required under the RMCP.

The Group must conduct EDD on all clients who are deemed to be high-risk.

Agreed standards may require us to consult other lists of entities and/or individuals.

The group must maintain principles and methodologies to ensure that prospective or existing business relationships or Single Transactions that do not appear to be legitimate are managed

appropriately. This may result in the declining, terminating or reporting of a business relationship, Single Transaction or activity.

4.6 Know your client

The Group must establish and verify the identity of all clients in line with agreed standards.

A risk-based approach may be followed in line with guidelines from the Group Chief AML, CFT and Sanctions Officer.

4.7 Client take-on requirements

The Group must not establish business relationships or conclude Single Transactions with clients:
- who would expose the Group to reputational, operational or legal risks due to non-compliance with its RMCP or any regulation associated with its RMCP;

- who insist on anonymity or who give fictitious names;
- who are oral trusts of which have not been reduced to writing;
- who are CAPS or
- who are shell banks.

4.8 Screening of domestic prominent influential persons and foreign prominent public officials

The group is obliged to identify if a prospective or existing client, associated party or beneficial owner is:

- a DPIP or FPPO;
- an immediate family member of a DPIP or FPPO; or
- a known close associate of a DPIP or FPPO,
- to assess the ML, TF, PF and Sanctions risk introduced as a result of establishing the business relationship.

The Group will screen prospective or existing clients, associated parties or beneficial owners against the Group's approved DPIP and FPPO lists prior to establishing a business relationship with the client.

In addition, the Group must screen all clients, associated parties and beneficial owners records on an ongoing basis and when any additions, amendments or deletions are made to the Group's approved DPIP and FPPO lists or identified party records.

4.9 Screening of individuals, entities, countries, goods and activities against sanctions lists and internal lists

The Group will screen prospective and existing client records and cross-border transactions by comparing prospective and existing client information and/or cross-border transaction details against the Group ratified sanctions lists, identified internal lists and the DNE list.

4.10 Reviewing matches

When a prospective-client, existing-client or cross-border transaction match is identified during the screening process, the party information or cross-border transaction must be reviewed and investigated to determine whether or not it is a false positive or a true positive.

4.11 Prohibitions and permitted financial services relating to sanctions listed individuals, entities, goods or activities

The Group must, where required, refuse to establish a new business relationship, continue with an existing business relationship or conclude a single transaction or a transaction in the course of a business relationship where a true positive match is identified in respect of:

- a specified entity identified in a notice issued by the President of the Republic of South Africa under section 25 of the Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004 (POCDATARA); and/or
- a person or an entity identified pursuant to a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1) of the Financial Intelligence Centre Ac, 38 of 2001, as amended (FICA),

unless that business relationship or transaction is a permitted financial service or permitted dealing of property.

The Group must, where required, refuse to facilitate a transaction where a true positive match is identified in respect of an individual or entity or activity or good listed on a ratified sanctions list if that facilitation would be in breach of the applicable sanctions regime.

4.12 Prohibitions and permitted transactions relating to individuals or entities listed on internal lists of the group

The Group must, unless approved by the Group Reputational Risk Committee (GRRC), refuse to establish a new business relationship, or conclude a Single Transaction with an individual or entity listed on the Group's DNE list.

The Group must, where required, escalate a transaction where a true positive match is identified in respect of an individual/ entity/ country/ industry listed on an internal list where such facilitation would be in breach of the applicable internal list requirements.

4.13 Reporting of individuals or entities identified on sanctions lists and internal lists

The Group must report the true positive match of any client or cross-border transaction identified on any ratified sanctions/ internal lists to the relevant internal reporting structures.

4.14 Declining or terminating business relationships or transactions

The Group may decline or terminate business relationships or single transactions where the ML, TF, PF and/or sanctions risk presented by the client falls outside the Group's risk appetite.

4.15 Notifying a client

The decision to notify a client must be taken in accordance with the facts and circumstances of each case. As a basic principle, the Group should seek to notify the client of a prohibition in relation to sanctions obligations as soon as practicable after the action has been taken.

4.16 Circumvention of sanctions

The Group must prohibit and detect attempts to circumvent sanctions.

4.17 Cash threshold reporting

The Group must, within two (2) business days after becoming aware of the reportable transaction, report to the Financial Intelligence Centre ("FIC") the prescribed particulars concerning a cash transaction or aggregate of cash transactions within a 24-hour reporting period, concluded with a client if in terms of the transaction(s) an amount of cash in excess of the prescribed amount is paid by the Group to the client, or to a person acting on behalf of the client, or to a person on whose behalf the client is acting, or received by the Group from the client, or from a person acting on behalf of the client, or from a person on whose behalf the client is acting.

4.18 Reporting of individuals or entities identified on sanctions lists and/or any property associated with individuals or entities designated for terrorist activity or in line with a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1) of Financial Intelligence Centre Act, 38 of 2001

The Group must within five (5) business days after becoming aware of a reportable transaction report to the FIC the prescribed details concerning any property, which it has in its possession or under its control, which is owned or controlled by or on behalf of or at the direction of:

- a specified entity identified in a notice issued by the President under section 25 of POCDATARA; or
- a person or an entity identified in line with a resolution of the Security Council of the United Nations contemplated in a notice referred to in section 26A(1) of FICA.

4.19 Suspicious and Unusual Transaction or Activity Report and Terrorist Financing Transaction or Activity Report The Group is obliged to report knowledge or suspicion in relation to:

- a transaction or series of transactions; and
- activity where no transaction is concluded,
- related to the proceeds of unlawful activity, ML, TF, PF or financial sanctions.

The Group is obliged to cooperate with the relevant authorities and release to them such information as required related to the proceeds of unlawful activity, ML, TF, PF or financial sanctions.

4.19.1 Period for reporting

The group must, within 15 business days of becoming aware of the reportable transaction, report to the FIC the prescribed details concerning knowledge or suspicion with regard to:

- a transaction or series of transactions; and
- activity where no transaction is concluded,
- related to the proceeds of unlawful activity, ML, TF, PF or financial sanctions.

4.19.2 No application of risk-based approach in the case of suspicious and unusual transactions or activities

Irrespective of the risk-based approach applied to the establishment, and ODD, of a business relationship or conclusion of a Single Transaction, the Group is not exempt from other relevant risk management obligations (eg suspicious-activity reporting) in respect of those business relationships or Single Transactions.

4.20 International electronic funds transfer reporting

The Group must, within the prescribed period report to the FIC all electronic transfers of funds, received from outside of the Republic or sent from the Republic. [Note: effective date to be advised]

4.21 Failure to report

Where an employee becomes aware of a reporting failure (inclusive of late reporting), the employee must inform the Group Chief AML, CFT and Sanctions Officer of the reporting failure immediately to ensure that the notification, where necessary, as per Directive 3/2014 is sent to the FIC.

4.22 Inclusion of sanctions and proliferation finance obligations in credit agreements

The Group will ensure that credit agreements make provision for the prohibition of clients making any of the finance provided by the Group available to sanctioned individuals/ entities or for the purposes of proliferation of weapons of mass destruction and sanctioned goods and/or activities.

4.23 United States citizens or residents

Where the Group employs a United States ("US") citizen or resident in a senior decision-making position, caution needs to be applied. US citizens or residents must have no capacity to approve, facilitate or process payments or business relationships with any individual, entity or country on a US sanctions list. If they do, the Group risks prosecution for a sanctions breach under the extraterritorial provisions of the United States of America ("USA") Patriot Act.

4.24 Recordkeeping

All CDD information and documentation, transactional information (including transaction monitoring, where applicable), client screening, external reporting and employee training records must be retained by the Group.
All records of prospective clients, existing clients or cross-border transactions related to sanctions risk and internal list management must be retained by the Group.

The applicable agreed standard will prescribe what records must be retained, the quality of records to be kept and the retention periods for those records.
Authorised employees must be able to retrieve and produce records that are required, in line with agreed standards and within periods set out in agreed standards.

4.25 Training

The group must provide, and employees are obliged to undergo, appropriate ongoing training on AML, CFT, CPF and sanctions risk management.

4.26 Coordinated Assurance, Compliance Monitoring and Independent Assurance

The Group must monitor and ensure:

- adherence to this policy;
- compliance with its obligations in terms of agreed standards;
- business units manage their respective businesses within the RMCP; and
- a coordinated approach in assessing and monitoring risks related to AML, CFT, CPF and sanctions.

Level 1 Policy for Anti-money-laundering, the Combating of the Financing of Terrorist and Countering of Proliferation Financing and Related Activities and Sanctions

Ref: Trevor Adams, 2022

NEDBANK

4.27 Awareness and communication

Employees must be made aware of the contents of this policy, which includes communication regarding their responsibilities and actions expected of them.

Employees must be made aware of the contents of the relevant local policy for AML, CFT, CPF and sanctions as implemented for their jurisdiction, which includes communication regarding their responsibilities and actions expected of them.

4.28 Roles and responsibilities for AML, CFT, CPF and Sanctions

The Group must clearly define ownership, accountability and responsibility across the three Lines of Defence pertaining to ML, TF, PF and Sanctions risk management.

4.29 Management reporting

Management reports must be produced to allow the Group to actively and effectively monitor initiatives and risks relating to ML, TF, PF and sanctions. These reports are to address the requirements of the various authorities and Group structures.