Group Compliance and Legal

Compliance, AML and Legal Risk Policy

Version No	3.0
Risk Owner	Group General Counsel and Chief Compliance Officer
Recommended by:	Group Management Risk Committee
Reviewed by:	Group Risk, Social and Ethics Committee
Review Date	21 October 2020
Level 1 Approved by:	LHL Board of Directors
Level 2 Approved by:	Group EXCO
Approval Date	TBA
Effective Date	TBA
Next Review Date	TBA

Confidentiality

This Compliance Risk Policy has been issued strictly for internal business purposes of Letshego Holdings Limited (LHL).

Restrictions

This policy is proprietary and is owned by LHL. All the information and images contained in this policy are the property of LHL unless otherwise indicated. The information it contains is confidential. This information is intended for internal use only by employees of LHL and may only be used in connection with the business in line with the Group's guidelines.

By accessing this policy you agree to be bound by all of the above terms and conditions.

None of the information or images contained in this document may be copied, reproduced, republished, downloaded or distributed either in whole or in part to any person or entity outside LHL except with the express permission in writing from an authorised representative of the Group.

Table of Contents

1. Introduction

1.1 Policy Statement

1.1.1 Letshego Holdings Limited (''the Group'') aspires to comply fully with all applicable laws, regulations and rules that govern its business both in Botswana and all the countries in which it operates.

1.1.2 This Compliance, AML and Legal Risk Policy supports the Group Compliance Risk Framework (a sub-framework of the Group ERM Framework) and contains all Compliance, Legal, Anti-Money Laundering (AML), Countering the Financing of Terrorism and Proliferation (CFT&P) and Sanctions related policies.

1.1.3 The Group is committed to sustaining a secure and robust financial system. This commitment is expressed through awareness of its responsibilities and being cognisant of local and international efforts to manage risks arising from Anti-money laundering (AML), countering the financing of terrorism and proliferation (CFT&P) and Sanctions (collectively AML / CFT&P and Sanctions). Effective supervisory oversight supported by prudent management of money laundering (ML), terrorist financing (TF) and Sanctions risks, is fundamental in ensuring the security and stability of financial institutions as socially responsible corporate citizens, as well as for the preservation of the integrity of the local and international financial systems.

1.1.4 The Compliance, AML and Legal Risk Policy is based on principles and must be ready in conjunction with the Compliance Risk Framework. It is supported by the Group Compliance Risk Standards, AML / CFT&P and Sanctions Guidelines, Compliance Risk Manual and various Group Procedures/ Processes.

1.1.5 In line with the Group ERM Framework, the Compliance, Legal, AML/CFT&P and Sanctions related policies are all categorized as Level 1 Policies as shown in Table 1 below. Level 1 Policies are approved by the Board and Level 2 Policies by Group EXCO.

Table 1: Compliance, AML and Legal Risk Policies

Item No.	Policy Name	Source
Compliance, AML and Legal Risk Policies		
1.	Compliance Risk Policy	Regulatory
2.	AML, Counter Terrorism and Proliferation Financing Policy	Regulatory
3.	Customer Acceptance Policy	Regulatory
4.	Gifts and Entertainment Policy	Regulatory
5.	Conflict of Interest Policy	Regulatory
6.	Agreements and Litigation Policy	Legal
7.	Legal Risk Principles Policy	Legal

1.2 Purpose of this Policy

1.2.1 The main purpose of this policy is to:

1.2.1.1 Ensure that the Group and its subsidiaries establish principles in compliance risk management including AML/CFT&P and comply fully with the letter and spirit of all applicable laws, regulations and rules in the countries in which the Group operates.

1.2.1.2 Enable the Group and its subsidiaries to manage legal risk proactively in order to avoid unacceptable risk and mitigate risk within acceptable levels.

1.2.1.3 Define circumstances under which the Group and its subsidiaries would not accept a new business relationship or would terminate an existing one in a consistent and structured manner.

1.2.1.4 Establish and regulate the receiving and giving of gifts and entertainment in order to prevent conflict of interest, undue influence or corruption of staff members, clients or potential clients, or service providers.

1.2.1.5 Promote ethical handling of actual, apparent or perceived conflicts of interests between personal and Group relationships Staff and Board Members.

1.3 Scope and compliance

1.3.1 This policy is applicable to all permanent staff including temporary staff, independent contractors, sub-contractors and agents of the Group and its subsidiaries.

1.3.2 Non-compliance with this policy may result in disciplinary action. Any exceptions to this policy must be approved by the Group General Counsel and Chief Compliance Officer in concurrence with the Group Chief Risk Officer and the Group Chief Executive and must be tabled at the next Group Risk, Social and Ethics Committee meeting for ratification as the dispensation will be related to Level 1 Policies.

2 Roles and Responsibilities

2.1 The Board of Directors

2.1.1 In addition to the Board's responsibilities outlined in the Compliance and Legal Risk Framework, the Board is ultimately responsible for Compliance, Legal risk management, Anti-Money Laundering (AML), Countering the Financing of Terrorism and Proliferation (CFT&P) and Sanctions (AML / CFT&P and Sanctions) for the Group and approves the policies and risk appetite.

2.1.2 All policies under the Group Compliance and Legal Policy are level 1 Policies and are approved by the Board. The Board has delegated the approval of Compliance and Legal Risk Standards and Guidelines, AML/CFT&P and Sanctions Guidelines to Group EXCO as the documents are needed to state the manner in which AML / CFT&P and Sanctions is conducted within the Group.

2.1.3 Furthermore, the Board is required to approve the Group Compliance and Legal Strategy each year as part of the overall Group Risk Strategy that supports the Business Strategy and Vision.

2.2 Group Risk, Social and Ethics Committee

2.2.1 The Committee is responsible for overseeing the implementation of the Compliance, Legal, Anti-money laundering (AML), Countering the Financing of Terrorism and Proliferation (CFT&P) and Sanctions policies including ensuring that compliance and anti-money laundering issues or activities are resolved effectively and expeditiously.

2.2.2 The Committee must review all Compliance, Legal, AML/CFT&P) and Sanctions policies and the related risk appetite before recommending them for approval by the Board.

2.2.3 The Committee must review on a quarterly basis Compliance, Legal, AML/CFT&P) and Sanctions reports submitted by the Group General Counsel and Chief Compliance Officer as part of the Group Risk reports and make appropriate decisions before recommending any approvals to the Board.

2.3 The Group EXCO

2.3.1 The Committee is responsible for approving the Compliance Risk Standards, AML/CFT&P) and Sanctions Guidelines whilst the related procedures/processes are delegated to the Group Management Risk Committee for approval in line with the Group ERM Framework.

2.3.2 The Committee ensures that all audit related issues as well as risk assessment findings are actioned appropriately and on a timely basis.

2.4 Group Management Risk Committee (GMRC)

2.4.1 The Committee shall approve all Compliance, Legal and AML/CFT&P) and Sanctions related procedures and processes in the Group.

2.4.2 The Committee shall review all Compliance, Legal and AML/CFT&P) and Sanctions Policies and recommend to the Board and for approval including risk appetite. Standards and Guidelines shall be recommended to Group EXCO for approval.

2.5 Policy Owners

2.5.1 The Policy Owners of Compliance, Legal and AML/CFT&P) and Sanctions risk must participate in the development and review of the policies before they are accepted by the Group Management Risk Committee and approved by the Board.

2.5.2 Policy Owners must ensure that Standards, Guidelines and Procedures/processes are developed to support the policies, where necessary.

2.5.3 Policy Owners must ensure that Compliance, Legal and AML/CFT&P) and Sanctions related policy implementation plans are developed and actioned as part of embedding risk activities in the day to day operations of the Group.

2.5.4 Submit any policy exceptions to the Group General Counsel and Chief Compliance Officer to agree with the Group Chief Risk Officer before final approval by the Group CEO and tabling for ratification at the next Group Risk, Social and Ethics Committee meeting.

2.5.5 Ensure the policies are reviewed biennially (every two years) and submitted to the Group Chief Risk Officer for sign off in concurrence with Group Compliance and Legal before recommending them to GMRC.

2.5.6 Risk Owners must also ensure that the policy intention remains relevant to the operations of the Group.

2.6 Control Owners

2.6.1 Control Owners must ensure that there are adequate controls to support the policies and the Compliance Risk Registers are updated on a monthly basis.

2.6.2 Update the Control Library for the department/function and participate in the annual risk assessment.

2.6.3 Responsible for closing outstanding Compliance, Legal and AML/CFT&P) and Sanctions internal and external audit items and ensure that every audit finding is entered in the departmental Risk Register including items from the Risk and Control Risk Assessment.

2.7 Group Compliance and Legal Risk Function

2.7.1 Reviews Policies, Standards, Guidelines and Procedures/Processes prior to approval for conformance to legal and regulatory requirements before submitting the same to the Group Chief Risk Officer for sign off and submission to Group Management Risk Committee.

2.7.2 Provides support, guidance and training to Policy, Control Owners and all staff, as required.

2.7.3 Reviews group policies for compliance with this policy, prior to approval.

2.7.4 Ensures that Compliance Risk Monitoring Plans are in place for key regulatory requirements.

2.7.5 Conducts Compliance Risk Monitoring Reviews on a quarterly basis and share the results with the Group Chief Risk Officer to ensure effective monitoring of Compliance, Legal and AML/CFT&P) and Sanctions risks across the Group.

2.7.6 Line Management

2.7.7 Line Management is responsible for implementation of Compliance, Legal and AML/CFT&P) and Sanctions related policies and ensuring compliance with the Standards, Guidelines and Procedures/ Processes.

2.7.8 They are accountable to the policy owner for providing assurance regarding the implementation of and compliance with Policies, Standards, Guidelines and Procedures/Processes.

2.8 Staff

2.8.1 Staff is responsible for adhering to all Compliance, Legal and AML/CFT&P) and Sanctions related policies, standards and procedures as part of accountability for achieving Group objectives.

2.9 Group Internal Audit

2.9.1 Internal Audit provides Group EXCO and the Board Audit Committee with assurance on the adequacy and effectiveness of the Compliance, Legal and AML/CFT&P) and Sanctions activities for the Group and its subsidiaries.

2.9.2 The Group Internal Audit rating for Group Compliance and Legal Function is taken as the main input into the Internal Control component of the overall departmental risk profile for the financial year.

Group Compliance and Legal Risk

Compliance and AML Risk Policies

3 Compliance and AML Risk Policies

3.1 Compliance Risk Policy

3.1.1 Rational and Scope

3.1.1.1 The purpose of this policy is to enable the Group to:

3.1.1.1.1 Comply fully with the letter and spirit of all applicable laws, regulations and rules in the countries in which the Group operates.

3.1.1.1.2 Establish principles in compliance risk management for the Group and its subsidiaries.

3.1.1.1.3 Monitor the compliance process in terms of consistency, adequacy and effectiveness, through participation and in coordination of the total compliance risk process within the Group and its subsidiaries.

3.1.1.1.4 This policy is applicable to all permanent staff including temporary staff, independent contractors, sub-contractors and agents of the Group and its subsidiaries.

3.1.2 Policy Minimum Requirements

3.1.2.1 The Group General Counsel and Chief Compliance Officer shall act as the Group Compliance Officer. However, the compliance function in countries will report to the Chief Risk Officers or the Chief Executive Officer where there is no Chief Risk Officer.

3.1.2.2 The Group Compliance Function must establish and maintain a Group Compliance Manual that supports this policy at operational level.

3.1.2.3 The Group Compliance function shall be independent of business activities, in order to discharge its responsibilities objectively.

3.1.2.4 The Group Compliance and Legal function including the in-country compliance functions must have appropriate standing and authority, the full co-operation and support of senior management and staff, the right to intervene in any transaction or project, and course of action where it has reason to believe a breach of laws, rules and standards or of internal compliance policies or procedures has occurred or might occur.

3.1.2.5 Depending on the country requirements, the regulator may be formally advised on both the appointment of the Group Compliance Officer and when he/she leaves employment including the reasons thereto.

3.1.2.6 All employees must be advised of the appointment of the Group Compliance Officer if required by regulation.

3.1.2.7 The Group Compliance Officer shall also assume the role of the Money Laundering Reporting Officer (MLRO) for the Group and the Chief Risk Officers or the CEOs in countries will act as the MLROs and liaise with the regulators. Where applicable, the regulator shall be advised accordingly.

3.1.2.8 A member of the Internal Audit Department of the Group or its subsidiaries must not perform the duties of the MLRO as this will create a conflict of interest.

3.1.2.9 This Compliance Policy is supported by the Anti-Money Laundering (AML) Policy, the Customer Acceptance Policy, procedures, systems and controls to combat money laundering and terrorist financing.

3.1.2.10 The Group and its subsidiaries must organize and control their affairs responsibly and effectively, with adequate risk management systems.

3.1.2.11 The Group must comply in its dealings with customers and with applicable consumer protection legislation. In addition, as a general principle, each subsidiary must pay due regard to the interests of its customers and treat them fairly.

3.1.2.12 Each subsidiary's communications with clients must comply with any requirements applicable to marketing or similar material in the jurisdictions in which it is prepared and disseminated.

3.1.2.13 The Group and its subsidiaries must handle customer complaints in accordance with applicable regulatory requirements.

3.1.2.14 The Group Compliance Officer must ensure that all levels of staff, including applicable contracted staff and Board members are made aware of prescribed legislative requirements, receive training required by legislation, as applicable and are trained and a record of such training kept.

3.1.2.15 The subsidiaries with specialized training requirements, must develop training programs that ensure compliance with prescribed legislative requirements.

3.1.2.16 The Group must put in place policies or controls to ensure that any significant outsourcing arrangements do not materially impair the quality of its internal controls or its ability to comply with its regulatory obligations.

3.1.2.17 The Group Compliance Function and the countries must develop and implement Compliance Risk Monitoring Plans (CRMP) for all key statutory and regulatory requirements (such as the Financial Intelligence Act) that have a significant impact on the Group's operations.

3.1.2.18 The Group Compliance and Legal Function must conduct an independent risk based Compliance Risk Monitoring Review (CRMR) for all the statutory or regulatory requirements with significant impact to Group's operations using a CRMR Matrix at least on a quarterly basis and report non-compliance issues to Group Management Risk and Compliance Committee.

3.1.2.19 Compliance training for all business staff must be developed and delivered in accordance with agreed plan for the year.

3.1.2.20 The Compliance Function must be closely involved in all significant proposed business developments within the Group, including the introduction of new business products or activities and the establishment or acquisition of new legal entities.

3.1.3 Policy Owner

3.1.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer.

3.1.3.2 Any clarification or request for further information shall be channeled to the Group General Counsel and Chief Compliance Officer.

3.1.4 Related Documents

3.1.4.1 This Policy must be ready in conjunction with the Anti-Money Laundering Policy, Customer Acceptance Policy, New Products Policy, Outsourcing Arrangements Policy and External Communication Policy.

3.2 Anti-Money Laundering, Counter Terrorism and Proliferation Financing Policy

3.2.1 Policy Rational and Scope

3.2.1.1 The purpose of this policy is to:

3.2.1.2 Protect the reputation and integrity of the Group and its subsidiaries by taking all reasonable steps to prevent its use as a channel for money laundering or terrorist financing purposes.

3.2.1.3 It also establishes the principles that will enable the recognition, investigation and reporting of suspicious activity to relevant authorities.

3.2.1.4 The policy is applicable to all the Group functions and subsidiaries.

3.2.2 Policy Minimum Requirements

3.2.2.1 **Risk Philosophy and Governance**

3.2.2.1.1 The Group and its subsidiaries take a formal stand against money laundering and financing of terrorism.

3.2.2.1.2 Money laundering and terrorist and proliferation financing risk is managed at source in line with the Group's philosophy that risk is best managed at source.

3.2.2.1.3 The Group and its subsidiaries shall take a proactive approach towards the management of money laundering and terrorist financing risk.

3.2.2.1.4 The Board is ultimately responsible for the management of money laundering and terrorist financing risk and will provide oversight in this regard including the provision of appropriate strategies and resources.

3.2.2.1.5 The Group and its subsidiaries must establish an independent and permanent Anti-Money Laundering (AML) function which will report through the Group General Counsel and Chief Compliance Officer and Chief Risk Officers in countries.

3.2.2.1.6 The function is responsible for the identification, assessment, measurement, monitoring, reporting and controlling of money laundering and terrorist financing risk.

3.2.2.1.7 The AML function shall be subject to mandatory audit by the Internal Audit department at least once every calendar year.

3.2.2.1.8 Senior Management both at Group and subsidiary level shall collectively and individually promote a compliance culture against money laundering and financing of terrorism.

3.2.2.2 **Compliance Group Based Program**

3.2.2.2.1 All transactions of the Group and all transactions done through its subsidiaries will be subjected to independent monitoring by the AML function without any exemptions.

3.2.2.2.2 The Anti-Money Laundering (AML) function shall develop tools, procedures (including setting of appropriate AML monitoring limits per country requirements) as is appropriate to manage dynamic money laundering and terrorist financing risk.

3.2.2.2.3 All employees and officers of the Group and its subsidiaries are to be trained in AML.

3.2.2.2.4 The Group General Counsel and Chief Compliance Officer and the Chief Risk Officers in their respective countries, are required to take reasonable steps that AML training is conducted and that the training is appropriately customized for user needs in line with the risk based approach to money laundering and counter financing of terrorist risk management.

3.2.2.2.5 Records must also be kept of all training undertaken as well as suspicious and unusual transaction reports received and submitted to the authorities, where applicable. All records must be stored securely and be capable of being retrieved without delay.

3.2.2.2.6 Non-adherence with this policy has severe repercussions and penalties, not only on the staff members concerned, but on the Group as a whole.

3.2.2.3 **Suspicious and unusual transaction reporting and co-operation with related authorities**

3.2.2.3.1 The Group must report all confirmed suspicious and unusual transactions to the appropriate authorities, where required by local regulations and will co-operate with the authorities to the extent permitted by applicable customer confidentiality obligations. This will be done in accordance with the regulatory requirements of each country.

3.2.2.3.2 Any staff member who has made or intends to make a suspicious transaction report must not discuss their suspicions with anyone other than their line manager, the compliance staff within the Group or the Money Laundering Reporting Officer (as appropriate).

3.2.2.3.3 Under no circumstances should the report be discussed with the customer or any other staff member. This is to avoid any risk of "tipping off" any person who is or may be involved in money laundering or terrorist financing activities.

3.2.2.3.4 Procedures must be put in place, where practical, to monitor a customer's activity against their profile.

3.2.2.3.5 Any activity that appears unusual when compared with their profile must be reviewed by the staff member responsible for the transaction, or the staff member responsible for the customer relationship to determine whether the circumstances give rise to any suspicion of money laundering or terrorist financing activity. If circumstances give rise to such a suspicion, a suspicious transaction report must be completed.

3.2.2.4 **Due Diligence**

3.2.2.4.1 Provide an enhanced due diligence service in relation to higher risk funders, partners, and clients within the Group and its subsidiaries.

3.2.2.4.2 Business, where not all of the required information can be obtained, will be declined.

3.2.2.4.3 Due diligence exceptions may only be permitted where indicated by law. Such exceptions in countries will only be signed off by the Chief Risk Officers or their representatives and reasons for the information or documentation not being available stated thereof on a Waiver Form. In no instances shall identity documents be waived.

3.2.2.5 **Prominent Influential Persons (Politically Exposed Persons) (PIP/PEP)**

3.2.2.5.1 The decision to open an account for PIP/PEP must be authorized by the Chief Risk officer in country.

3.2.2.5.2 All PEP/PIP relationships must undergo an annual PIP/PEP Acceptance review.

3.2.2.6 **Monitoring Transactions for Staff Members**

3.2.2.6.1 Where applicable, the AML Function shall monitor staff accounts as a separate category and report to the Country Chief Executive Officer any suspicious activities/transactions.

3.2.2.6.2 For purposes of effective monitoring of staff accounts, the Group or subsidiary Human Capital Officer must furnish the Group or subsidiary Chief Risk Officer with a list of the declared business interest of all staff highlighting expected cash flows.

3.2.2.6.3 Such information is required to be submitted to the Group or subsidiary Chief Risk Officer immediately upon being submitted to the Group or subsidiary Human Capital Officer by staff.

3.2.2.7 **Completing the Annual AML/CTF Refresher Trainings**

3.2.2.7.1 Annually, the Board, Senior Management and all employees of the Group and its subsidiaries must complete the "Annual AML/CTF refresher training" and records are to be maintained by the AML Compliance Officer.

3.2.2.7.2 The Group General Counsel and Chief Compliance Officer and the Chief Risk Officers in their respective subsidiaries are required to take reasonable steps to ensure AML training is conducted and that the training is appropriately customized for user needs in line with the risk based approach to money laundering and counter financing of terrorist risk management.

3.2.2.7.3 Records must also be kept of all training undertaken as well as suspicious and unusual transaction reports received and submitted to the authorities, where applicable. All records must be stored securely and be capable of being retrieved immediately.

3.2.2.8 **Risk Based Approach**

3.2.2.8.1 By adopting a risk-based approach, it is possible to ensure that measures to prevent or mitigate Money Laundering or Terrorist and Proliferation financing are commensurate with the risks identified.

3.2.2.8.2 This allows resources to be allocated in accordance with the risks identified. The Group advocates a Risk-Based Approach to identifying and verifying prospective business partner, funders or customers. In this regard, the Group promotes the use of four levels of assessment to be applied, namely Low Risk, Medium Risk, High Risk and Prohibited.

3.2.2.9 **Prohibition of Business Relationships**

3.2.2.9.1 The Group may not enter into a business relationship or transact with customers who:

3.2.2.9.2 Provide fictitious names

3.2.2.9.3 Prefer to remain anonymous

3.2.2.9.4 Refuse to provide mandatory information

3.2.2.9.5 Are considered to be involved in criminal activities, terrorist or proliferation financing.

3.2.2.9.6 This section must be read in conjunction with the AML Guidelines for a detailed prohibition list.

3.2.2.10 **Board of Directors AML Roles and Responsibilities**

3.2.2.10.1 The Board of directors is ultimately responsible for AML/CFT&P and Sanctions compliance, but the responsibility to ensure that all the Group's activities comply with regulatory requirements is delegated to the Group Chief Executive as well as Group EXCO.

3.2.2.10.2 The Board has the duty to make the necessary enquires to ensure that the requisite systems, practices and culture are in place to manage all compliance risks to which the Group is exposed to.

3.2.2.10.3 There must be an appointed fit and proper person at managerial level to assist the Group, its subsidiaries, and employees in complying with AML, CFT and PF requirements.

3.2.2.11 **Group EXCO AML Roles and Responsibilities**

3.2.2.11.1 The day to day compliance with money laundering obligations within all segments of the Group for which they are responsible;

3.2.2.11.2 Ensuring that the AML Compliance Officer is provided with prompt advice of unusual/suspicious transactions and other matters of significance;

3.2.2.11.3 Seeking from the Compliance Desk, at least quarterly, a report relating to the Group's compliance with its anti-money laundering obligations and acting on the findings and recommendations.

3.2.2.12 **All staff members must:**

3.2.2.12.1 Be aware of their personal legal obligations as regards customer identification, customer acceptance, AML, and CFT requirements.

3.2.2.12.2 Be aware of the Group's Policies on KYC, AML & CFT and Compliance and follow the Group's procedures as provided thereof.

3.2.2.12.3 Be alert for anything suspicious.

3.2.2.12.4 Monitor customer activities and transactions.

3.2.2.12.5 Report suspicions in line with internal procedures.

3.2.2.12.6 Take personal ownership of mandatory KYC, AML & CFT training as provided for by the Group.

3.2.2.13 **AML Compliance Officer (AMLCO)**

3.2.2.13.1 The AML Compliance Officer as part of the Compliance Function, is responsible for identification, measurement, documentation, management and reporting of the Group's KYC, AML/CFT&P and Sanctions risk;

3.2.2.13.2 To independently monitor client and staff transactions;

3.2.2.13.3 To maintain a Register of High Risk Clients and conduct enhanced monitoring of such clients including monitoring of their transactions and activities.

3.2.2.13.4 To identify risk factors and appropriately categorise clients by developing and reviewing the Customer Due Diligence Matrix;

3.2.2.13.5 To communicate to all staff an updated Customer Due Diligence Matrix at least annually or confirm thereof if there is no fundamental change in the components of the matrix;

3.2.2.13.6 To conduct at least annual independent identification of PEPs and update the Central PEPs Register and communicate to senior management thereof;

3.2.2.13.7 To conduct periodic independent sanction screening for all clients as is necessary;

3.2.2.13.8 To train all staff on AML, CFT and KYC and develop specialized training material for departments with specific training needs.

3.2.2.13.9 To keep a Mandatory AML, CFT and KYC Compliance Training Register and ensure that all staff are trained within 3 months of being employed by the Group whether on contact, fixed term or permanently.

3.2.2.13.10 To ensure consistency on the Group's manuals and policies related to KYC, AML and CFT such as but not limited to the Account Opening Manual, Customer Acceptance Policy and Compliance Manual & Policy.

3.2.2.13.11 To ensure constancy between the regulatory requirements and internal policies & procedures. To this end, the AML, CFT and KYC Function shall review the relevant policies and/or procedures post any regulatory or statutory changes but shall in any event be reviewed at least annually and communicated to all relevant staff thereof;

3.2.2.13.12 Ensuring that all segments of the Group are complying with the AML, CFT and KYC policies;

3.2.2.13.13 Periodic reporting to the Board, Senior Management and Group on AML, CFT and KYC issues respectively;

3.2.2.13.14 Undertaking the internal review of all suspicions transactions reports and determining whether such suspicions have substance and require disclosure.

3.2.2.13.15 Obtaining and making use of national and international findings concerning countries with serious deficiencies;

3.2.2.13.16 To review compliance by the Group with money laundering, terrorist and proliferation financing statutory and regulatory obligations, in respect of the Group's money laundering policy and procedures.

3.2.2.13.17 Keep a register of all internal reports received and external reports made to the authorities.

3.2.2.13.18 Implement effective controls to guard against "tipping off" any person who is or may be involved in ML/TF & PF activities.

3.2.2.13.19 The AML Compliance Officer shall circulate to all staff persons listed on sanctions list as observed by the Group as may be necessary;

3.2.2.13.20 AML Compliance Officer shall monitor on a daily basis any additions or removals to the sanctions list and circulate such additions to all staff immediately upon noticing any such additions or removal as may be necessary;

3.2.2.13.21 All accounts shall be subjected to sanctions screening before the account is opened;

3.2.2.13.22 In line with the Group's policy, the Group will refer to Consolidated United Nations Security Council Sanctions List, Office of Foreign Assets Control (OFAC) Specially Designated Nationals & Blocked Persons Sanction List and European Sanctions List for purposes of sanction screening;

3.2.2.13.23 Furthermore, the AMLCO may indicate other persons to be screened by way of a circular to all staff.

3.2.2.14 **Internal Audit AML Related Roles and Responsibilities**

3.2.2.14.1 Group Internal Audit (GIA) provides independent assurance on the adequacy and effectiveness of the processes that support this policy.

3.2.2.14.2 GIA provides an oversite and monitoring role for all AML systems, controls and processes, ensuring the Group's compliance to regulatory requirements.

3.2.3 Policy Owner

3.2.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer.

3.2.3.2 Any clarification or request for further information shall be channeled to the Group General Counsel and Chief Compliance Officer via e-mail or other forms of communication.

3.2.4 Related Documents

3.2.4.1 This policy must be read in conjunction with the following:

- AML/CFT&P and Sanctions Guidelines
- Customer Acceptance Policy
- Compliance Risk Policy and the Compliance Manual
- Financial Intelligence Act (2018)
- Financial Intelligence Regulations (2018)
- Counter Terrorism Act (2018)
- Compliance Risk Framework

3.3 Customer Acceptance Policy

3.3.1 Policy Rational and Scope

3.3.1.1 This policy provides a consistent mechanism of identifying customers and profiling them into appropriate risk categories as per the Group's risk assessment on money laundering and financing of terrorism risk.

3.3.1.2 The policy further defines circumstances under which the Group and its subsidiaries would not accept a new business relationship or would terminate an existing one in a consistent and structured manner.

3.3.1.3 It also provides direction as regards keeping of customer records and related documentation.

3.3.1.4 The policy is applicable to all Group functions and subsidiaries.

3.3.2 Policy Minimum Requirements

3.3.2.1 **Customer Identification**

3.3.2.1.1 The Group and its subsidiaries must use a consistent process to ascertain and verify the identity of all customers. Each customer account is to be assigned an account owner who will be responsible for managing the customer identification and categorization process initially and on a continuous basis.

3.3.2.1.2 The Group and its subsidiaries must not establish a business relationship with a customer who cannot provide evidence of their identity.

3.3.2.1.3 The identity of any beneficial owners other than the customer must be ascertained and verified. The authority of persons acting on behalf of others must be established and verified. The Group may request further information above the minimum for the customer or product category should a reasonable basis be noted including suspicion of money laundering or financing of terrorism.

3.3.2.1.4 Each product type and customer type shall have minimum identity requirement established in line with regulatory requirements.

3.3.2.1.5 The minimum information required for each prospective client must include:

3.3.2.1.5.1 Relevant information pertaining to the client's background.

3.3.2.1.5.2 The client's country of origin and residence;

3.3.2.1.5.3 any linked accounts that the client or any other party, to the business relationship or single transaction, may have at that institution;

3.3.2.1.5.4 the nature and location of the client's business activities, as well as the nature and source of personal income and;

3.3.2.1.5.5 Any other information that may assist the Group to determine whether the business relationship with the client may be vulnerable to the laundering of the proceeds of corruption or any other crime.

3.3.2.2 **Customer Acceptance**

3.3.2.2.1 The Group and its subsidiaries will only enter into a business relationship with a prospective customer post appropriate categorization of the customer as per the Group's Customer Due Diligence Matrix.

3.3.2.2.2 The Group shall categorize potential customers or customers into one of the four categories outlined in the section below prior to establish a business relationship. The categorization of customers is to be viewed as continuous process and a proactive approach must be taken.

3.3.2.2.3 Each business relationship is to be established with an assigned account manager who will be responsible for managing the customer categorization process initially and on a continuous basis.

3.3.2.2.4 The categorization of customers is on a case by case basis taking into account the risk factors noted as per the Customer Due Diligence Matrix.

3.3.2.2.5 The Group shall categorize customers into one of the following four categories namely prohibited, high risk, medium risk and low risk categories.

3.3.2.2.6 The Group and its subsidiaries must not tolerate any dealings of any kind with clients in the prohibited category given the risk and consequently no business relationship shall be established nor a single transaction conducted for customers falling into this category.

3.3.2.2.7 Prohibited customers include: anonymous accounts; Shell banks; persons listed on

3.3.2.2.8 Consolidated United Nations Security Council Sanctions List, Office of Foreign Assets Control

3.3.2.2.9 (OFAC) Specially Designated Nationals & Blocked Persons Sanction List and European

3.3.2.2.10 Sanctions List; and any persons notified to employees, management and officers of the Group and its subsidiaries by the Money Laundering Reporting Officer by way of a circular.

3.3.2.3 **Record Keeping**

3.3.2.3.1 Customer financial records shall be retained for a minimum of 5 years from date of transaction whilst non-financial records such as identity records shall be retained for a minimum of 5 years from date of termination of relationship as per regulatory requirements and in a consistent and structured manner.

3.3.2.3.2 The same 5 year retention period is applicable to related documents such as suspicious transactions reports and account categorization documents from date of termination of the relationship with the client.

3.3.3 Policy Owner

3.3.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer.

3.3.3.2 Any clarification or request for further information shall be channeled to the Group General Counsel and Chief Compliance Officer via e-mail or other forms of communication.

3.3.4 Related Documents

3.3.4.1 This policy must be read in conjunction with the Anti-Money Laundering Policy, Compliance Risk Policy, KYC and AML Procedures.

3.4 Gifts and Entertainment Policy

3.4.1 Rational and Scope

3.4.1.1 The purpose of this policy is to regulate the receiving and giving of gifts and entertainment in order to prevent conflict of interest, undue influence or corruption of staff members, clients or potential clients, or service providers when making decisions in order for the Group and its subsidiaries to gain unfair commercial advantage.

3.4.1.2 It also ensures that stakeholders are made aware of their obligations in terms of the applicable legislation and internal rules, including internal reporting procedures to ensure that all gifts and entertainment are reported and recorded.

3.4.1.3 This policy applies to all staff members of the Group and its subsidiaries.

3.4.2 Policy Minimum Requirements

3.4.2.1 Staff members may give, or accept, or receive appropriate, lawful gifts and entertainment in connection with the Group engagements with clients/customers or potential clients/customers, service providers, or business-related third parties and other governmental or non-governmental parties, provided that all such gifts and entertainment are nominal in value and not offered, given or received with the intent or prospect of influencing the recipient's business decision-making.

3.4.2.2 Attempts by suppliers, clients or third parties to solicit gifts and/or entertainment from a staff member must be reported immediately to the Whistle Blower Hotline/ Compliance Department.

3.4.2.3 No staff member may give or receive gifts and entertainment that violate the law, regulations, agreements or reasonable customs of the marketplace/normal business practices.

3.4.2.4 Staff members must be aware of cultural sensitivities when giving, accepting or receiving gifts and entertainment.

3.4.2.5 Openness and transparency in terms of this policy must be encouraged at all times.

3.4.2.6 Due care must be exercised at all times in the giving, or acceptance of gifts and entertainment.

3.4.2.7 A staff member is prohibited from offering, soliciting, accepting or receiving any gifts and entertainment directly or indirectly from client/customer or potential client/customer, service provider, or business-related third party, or government and/or public body official other than in terms of this policy.

3.4.2.8 A staff member's family is prohibited from offering, soliciting, accepting any gift or entertainment directly, or indirectly, where such gifts and entertainment are obtained from client/customer or potential client/customer, service provider, or business-related third party, or government and/or public body officials other than in terms of this policy.

3.4.2.9 Gifts and entertainment in the form of cash (for this purpose cash equivalent such as vouchers or gift cards, will be construed as being cash) can be accepted but must be declared, registered and retained only after appropriate clearance.

3.4.2.10 Staff members may not offer, or give, or accept, any gifts and entertainment where the offer may be perceived as intended to:

3.4.2.10.1 Persuade the staff member to perform or refrain from performing certain actions.

3.4.2.10.2 Potentially compromise or would be perceived to compromise the independence of the staff member.

3.4.2.11 All gifts and entertainment whose value is in excess of P$1000 (One thousand) must be promptly reported, in writing, to Compliance Department, and may not be accepted/given/received without the permission of the relevant line management. The gift must only be retained after appropriate clearance.

3.4.2.12 Where the value of the gift is unknown, the individual must estimate the value and declare to the Compliance function. Compliance function must validate the estimated amount.

3.4.2.13 The giving or acceptance of gifts and entertainment may not take place in circumstances that amount to a conflict of interest on the part of the staff member.

3.4.2.14 The giving and/or acceptance of gifts and entertainment may not take place in circumstances that amount to corruption, nor may the staff member give or receive gifts and entertainment where they may be perceived to amount to the exertion of undue influence in order to obtain business, benefit unduly or gain unfair commercial advantage on behalf of the Group or Subsidiary.

3.4.2.15 Entertainment received must be declared and recorded in the Gifts and Entertainment Register held by Compliance Department within five working days of such receipt, before acting on such receipt or making use of the gift.

3.4.2.16 All requests whether approved or not in terms of this policy, must be included in the Gifts and Entertainment Register.

3.4.2.17 Compliance Function must keep the Gifts and Entertainment Register in either a manual or electronic format for a minimum of three years.

3.4.2.18 This policy does not apply to the following:

3.4.2.18.1 Normal business lunches, office parties and business seminars, Group sponsored functions, promotions or hospitality events; or gifts and entertainment of nominal value or to promotional items of nominal value that display Letshego logo.

3.4.2.18.2 Payments or awards received by a staff member from Letshego or gifts and entertainment thus received in respect of anniversaries or other personal occasions - internal staff incentives must not be recorded in terms of this policy; and

3.4.2.18.3 Where there is a formal agreement between the Group and third parties for special rates for staff members, for example, items, goods, services, information - car rentals, medical aid, airlines, shuttle services and mobile phone services among others.

3.4.3 Policy Owner

3.4.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer.

3.4.3.2 Any clarification or request for further information shall be channeled to Group Compliance and Legal.

3.4.4 Related Documents

3.4.4.1 This policy must be read in conjunction with the Conflict of Interest Policy; Code of Conduct, Anti- Fraud and Corruption Policy, Whistle Blowing Policy and Human Resources Policies.

3.5 Conflict of Interest Policy

3.5.1 Rational and Scope

3.5.1.1 The main purpose of the conflict of interest policy is to promote ethical handling of actual, apparent or perceived conflicts of interests between personal and Group relationships.

3.5.1.2 The minimum requirements outlined in this policy apply to all employees and directors of the Group and its subsidiaries.

3.5.2 Policy Minimum Requirements

3.5.2.1 The Group endorses the principle that an employee (or director) must serve his or her employer honestly and faithfully. In that an employee:

3.5.2.1.1 Must devote his/her working hours to the employer's business and not conduct unauthorized business during working hours.

3.5.2.1.2 May not commence another business in competition with the employer or even attempt to make arrangements in this regard.

3.5.2.1.3 May not solicit the employer's customers or employees to build up his/her own business, and;

3.5.2.1.4 May not place himself in a position which may give rise to a conflict of interest as between himself or herself and his/her employer.

3.5.2.2 The Group and its clients, expect a "professional" employee to not only disclose their circumstances that may produce a conflict of interest, but to also recuse themselves from any decision making process in regard to the issue in question.

3.5.2.3 Any employee of the Group is prohibited from using his/her official position for personal gain.

3.5.2.4 An employee may not engage in work associated with the conduct of any enterprise or entity which may be in conflict with and/or disruptive to the employee's/director's duties with the Group.

3.5.2.5 An employee may not enter into any business transaction with or in conjunction with a client or supplier of the Group, without the prior written consent of the Group, other than in the ordinary course of business and on the same terms that are available to the general public.

3.5.2.6 An employee may not act as a director of a private or public company, a member of a closed corporation, a trustee of a business trust, or partner in partnership, which has dealings with the Group without prior consent of the Group. This excludes personal or family investments.

3.5.2.7 An employee shall disclose to the Group any personal financial interest he/she has, as well as any financial interests known to him/her of any immediate family members or business associates of the employee of the Group in any matter to be considered by the Group or in which another person or entity proposes to do business with the Group, other than in the ordinary course of business and on the same terms that are available to the general public.

3.5.2.8 Employees are occasionally invited to serve on external boards/trusts as non-executive directors/trustees. King IV recommends that executive directors should be encouraged to hold other non-executive directorship only to the extent that these do not interfere with their immediate management responsibilities. In such circumstances, the following conditions must be observed:

3.5.2.8.1 Any staff member is prohibited from accepting an appointment to serve on the Board of non-Group companies, unless written approval is obtained. This condition is not applicable where an employee serves on external board at the request of the Group.

3.5.2.8.2 The details of such invitation(s) must be submitted to the employee's manager, and for Group Executive Committee Members, to the Group General Counsel and Chief Compliance Officer.

3.5.2.8.3 Such a request must explain why the proposed appointment:

3.5.2.8.3.1 Is not in conflict with the interests of the Group;

3.5.2.8.3.2 Will not detrimentally affect the employee's contribution to the Group; and

3.5.2.8.3.3 Will be of benefit to the employee in terms of personal development or in terms of expanding the individual's circle of influence and contacts.

3.5.2.9 Approval of such a request is at the discretion of the employee's manager, and for members of Group EXCO, it will be at the Group Chief Executive's discretion, with due consideration of governance issues, the stakeholder engagements and potential reputational risk.

3.5.2.10 Group Human Capital must, by the end of the first quarter of each year, review such approval(s) to ascertain that the original intentions continue to exist.

3.5.2.11 The Group General Counsel and Chief Compliance Officer must monitor the process.

3.5.2.12 Any fees payable in terms of non-executive appointments must be paid directly to the Group. As there may be tax implications for individuals accepting such appointments, care must be taken in structuring arrangements so that there is not a double taxation of the remuneration of such fees.

3.5.2.13 If approval is granted for an external non-executive directorship/trusteeship, the external board and all other associated parties must be made aware that the director or employee has no authority to represent the Group in the matters pertaining to such board's/ trust's affairs.

3.5.2.14 The number of external boards on which employee/executive can serve will be determined by the Group Executive Committee or the Group Board where it concerns the Group Chief Executive.

3.5.3 Policy Owner

3.5.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer.

3.5.3.2 Any clarification or request for further information shall be channeled to Group General Counsel and Chief Compliance Officer.

3.5.4 Related Documents

3.5.4.1 The policy must be read in conjunction with the Code of Conduct, Gifts and Entertainment Policy, Whistle Blowing Policy and Human Capital Policies.

Group Compliance and Legal Risk

Legal Risk Policies

4 Legal Policies

4.1 Agreements and Litigation Policy

4.1.1 Rational and Scope

4.1.1.1 The purpose of this policy is to enable the Group to manage legal risk proactively in order to avoid unacceptable risk, mitigate risk within acceptable levels, and determine appropriate levels of legal risk appetite.

4.1.1.2 This policy covers the Group and its subsidiaries.

4.1.2 Policy Minimum Requirements

4.1.2.1 **Litigation**

4.1.2.1.1 The Group must use highly skilled external legal practitioners with good standing for all transactions out of the ordinary course of business to which it is a party.

4.1.2.1.2 A panel of legal practitioners, approved by Group EXCO, must be used. The panel must be referred to Group Compliance and Legal for noting before seeking Group EXCO or Country Management Committee for approval.

4.1.2.1.3 The Group General Counsel and Chief Compliance Officer must carefully consider the implications of any court action with respect to legal costs, image and reputational risks as well as the amount of management time required to bring the case to finality.

4.1.2.1.4 The Group General Counsel and Chief Compliance Officer or the Head of Department responsible for legal risk in-country must ensure that procedures relating to litigation are documented and maintained.

4.1.2.2 **Legal Advice**

4.1.2.2.1 In the ordinary course of business, the Group or subsidiaries' various units or departments must in the first instance seek legal advice from their respective Legal Function or Compliance and Legal department.

4.1.2.2.2 An in-country legal function must, with the concurrence of Group Compliance and Legal, refer the matter to an outside practitioner if it does not have the capacity and/or expertise to provide the requisite advice with the exception of collection matters that are in the ordinary course of business.

4.1.2.2.3 Legal advice must be sought for all transactions out of the ordinary course of business to which the Group or subsidiary are party to.

4.1.2.2.4 Such transactions must be referred to Group Compliance and Legal. Management must ensure that all legal risks have been identified, mitigated and that these risks are adequately managed and recorded.

4.1.2.2.5 Management shall further ensure that all the legal requirements pertaining to a subsidiary are adequately addressed where-after the subsidiary shall seek final sign-off on all legal documentation relating to or in connection with such transactions from Group Compliance and Legal on material legal matters that are 2% and above of Profit Before Impairments and Taxation (PBIT).

4.1.2.3 **Agreements**

4.1.2.3.1 The drafting of credit documentation and standard legal documentation shall not be referred to external practitioners without Group Compliance and Legal consent. The subsidiary will use documentation, which will be adapted by the legal function in country to cater for country specific legal requirements.

4.1.2.3.2 Documented signing authorities relating to agreements must be maintained.

4.1.2.3.3 The Legal Function or Head of Unit in-country responsible for legal risk shall maintain a register of all agreements entered into as well as a schedule of legal exposures.

4.1.2.3.4 An updated schedule of all litigious matters must be tabled at Group Management Risk Committee and the Group Risk, Social and Ethics Committee meetings.

4.1.2.4 **Loan and collateral documentation**

4.1.2.4.1 The Head of Unit responsible for legal risk in-country and the Group General Counsel and Chief Compliance Officer shall sign-off all standard loan and collateral documentation ("approved documentation") for individuals and Medium to Small Enterprise (MSEs) customers.

4.1.2.4.2 Unless material changes are effected to the approved documentation, these documents shall be used without further reference to Group Compliance and Legal Function.

4.1.2.5 **Credit legal risk**

4.1.2.5.1 Management must address the legal risks associated with the risk that assets, in the form of a monetary claim against a counterparty, may not result in a cash receipt (or equivalent) in accordance with the terms of the contract and in doing so, managing the legal risks inherent inter alia in lending, failure by a counterparty to perform in accordance with the terms and conditions of contract, settlement, the inability to realize full collateral value due to unforeseen legal or adverse market conditions and changes pertaining to any specific industry which has adverse legal consequences.

4.1.2.6 **Reporting**

4.1.2.6.1 The Group General Counsel and Chief Compliance Officer or the Head of Department responsible for legal risk in-country shall, at least quarterly, provide a comprehensive report on all significant legal risks to the Group Management Risk Committee or Management Risk Committee respectively.

4.1.2.6.2 The Group General Counsel and Chief Compliance Officer shall report all significant legal risks to the Group Risk, Social and Ethics Committee and the in country legal function will submit the same to the Board Audit and Risk Committee at least on a quarterly basis.

4.1.3 Policy Owner

4.1.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer and shall be adopted by all Group Functions and subsidiaries as a legal risk requirement.

4.1.3.2 Any clarification or request for further information shall be channeled to Group Compliance and Legal Function.

4.1.4 Related Documents

4.1.4.1 This policy must be read in conjunction with Credit Risk Policies, Operational Risk Policies, Reputational Risk Policies and Compliance Risk Policies.

4.2 Legal Risk Principles Policy

4.2.1 Rational and Scope

4.2.1.1 The purpose of this policy is to enable the Group or its subsidiaries to manage legal risk proactively in order to avoid unacceptable risk, mitigate risk within acceptable levels, and determine appropriate levels of legal risk appetite within the entity.

4.2.1.2 This policy covers the Group and its subsidiaries. It does not cover the Credit legal risk principles which are detailed in the Agreements and Litigation Policy.

4.2.2 Policy Minimum Requirements

4.2.2.1 **Strategic legal risk principles**

4.2.2.1.1 The Group and its subsidiaries must manage the legal consequences of actions taken in an ever-changing environment to prevent adverse and inappropriate results and in doing so, ensuring that the Group acknowledges and responds to the significantly increasing legal complexities and regulations in the financial industry.

4.2.2.2 **Enterprise-wide legal risk principles**

4.2.2.2.1 The Group and its subsidiaries must manage enterprise-wide risk by identifying areas of weakness that may have legal implications and reporting such areas to the correct departments so that they can be addressed.

4.2.2.2.2 Management must apply adequate strategy to manage legal risk across the Group which is aligned to its overall business strategy and key objectives and which is based on best practice.

4.2.2.2.3 The Board of Directors and senior management must be trained in the different legal risk areas that the Group or Subsidiary is exposed to, thereby reducing the level of risk governance.

4.2.2.3 **Operational legal risk principles**

4.2.2.3.1 Management must address the legal risk of loss resulting from inadequate or failed internal processes, people and systems and from external events such as external systems failure and civil or criminal litigation, and in doing so:

4.2.2.3.1.1 Address legal risks arising from business disruption and non-continuous service to Customers;

4.2.2.3.1.2 Manage legal risk associated with any criminal or civil activity which includes negligence, dishonesty, and non-adherence to procedures, policies and breach of security or fiduciary duties arising from contract of employment or common or statutory laws;

4.2.2.3.1.3 Address the risk of third party claims against the Group as a result of a negligent act, error or omission, a dishonest or fraudulent act or omission, breach of trust; or

4.2.2.3.1.4 Professional duty, misrepresentation and defamation, breach of client confidentiality, loss of client documents and failure to act or execute transactions on behalf of a client in accordance with an agreed mandate.

4.2.2.4 **Compliance legal risk principles**

4.2.2.4.1 Management must ensure that the Group or Subsidiary complies at all levels with laws, rules, regulations, internal policies and authority levels, prescribed practices and ethical standards and in doing so ensuring that the Group does not suffer any reputational damage and that it maintains a good relationship with its regulators.

4.2.2.5 **Reputational legal risk principles**

4.2.2.5.1 Management must ensure that the Group or subsidiary does not suffer loss of business or legal action as a result of an activity, action or stance taken by the Group or its officials which will impair its image in the communities in which it operates and the long term trust placed in the organization by its stakeholders, by making sure that:

4.2.2.5.1.1 Communications to clients and stakeholders are prepared in accordance with the relevant set of legal and regulatory guidelines, policies and client agreements/ mandates/ policies and are authorized, accurate and complete.

4.2.2.5.1.2 Good relations are maintained with governmental and regulatory bodies to ensure that the Group achieves its strategic and business objectives.

4.2.2.5.1.3 Information is disclosed adequately and timeously as required by law, regulations, and/or International Financial Reporting Standards (IFRS).

4.2.2.5.1.4 Direct all media queries to the Group Strategic Communications and not deal with the media outside of Strategic Communications Function approval.

4.2.2.6 **New Business legal risk principles**

4.2.2.6.1 Group Compliance and Legal must assist in all legal aspects pertaining to new solutions (products) and new business development, which includes legal aspects inherent in the structuring of new solutions and transactions. Address also the legal risks associated with providing inappropriate solutions to clients or potential clients that fail to meet legal requirements.

4.2.2.6.2 The Group Compliance and Legal sign-off of all new solutions (products) and business development is essential to ensure the requisite due diligence has been undertaken and where need be regulatory approvals are obtained.

4.2.2.6.3 Group Compliance and Legal is required to partake in the development of terms and conditions for new and existing products to ensure that relevant and minimum disclosures are met in line with internal and local regulatory best practice principles of treating customers fairly (TCF).

4.2.2.6.4 The in-country legal function must, with the concurrence of Group General Counsel and Chief Compliance Officer review the new solutions to align to in-country requirements.

4.2.2.7 **Information technology legal risk principles**

4.2.2.7.1 Management must address legal risks resulting from system malfunction and unavailability, security breaches and inadequate systems in general and in doing so, addressing the unique legal risks arising from its business solutions initiatives, such as new solution development, access security, information security and confidentiality, third party legal liability and legislative and regulatory requirements.

4.2.2.8 **People legal risk principles**

4.2.2.8.1 Management must ensure that employees have the necessary skills, experience, training and attributes to perform their work effectively, and that employees comply with the organizational culture.

4.2.2.8.2 Group Compliance and Legal must ensure that employees and all internal stakeholders are sensitized and become aware of their legal obligations.

4.2.3 Policy Owner

4.2.3.1 This Policy is owned by the Group General Counsel and Chief Compliance Officer and shall be adopted by all Group Functions and subsidiaries as a legal risk requirement.

4.2.3.2 Any clarification or request for further information shall be channeled to Group General Counsel and Chief Compliance Officer.

4.2.4 Related Documents

4.2.4.1 This policy must be read in conjunction with Credit Risk Policies, Operational Risk Policies, Reputational Risk Policies and Compliance Risk Policies.

END

Appendix 1: Definition of Terms

Term	Description
Money laundering	Money laundering involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities. In other words, money laundering is the process of making dirty money look clean. Drug traffickers, armed robbers, terrorists, illegal arms dealers, fraudsters, human traffickers and tax evaders are common drivers of money laundering.
Placement (Injection or Pre-washing)	The physical disposal of cash or other assets derived from criminal activity. During this initial phase, the money launderer introduces the illegal proceeds into the financial system.
Layering (Stacking or Washing)	The separation of illicit proceeds from their source by layers of financial transactions intended to conceal the origin of the proceeds. This stage involves converting the proceeds of the crime into another form and creating complex layers of financial transactions to disguise the audit trail, source and ownership of funds.
Integration (Recycling)	Supplying apparent legitimacy to illicit wealth through the re-entry of the funds into the economy in what appears to be normal business or personal transactions.
Terrorist and Proliferation Financing	Terrorist Financing is the process by which terrorists fund their operations in order to perform terrorist acts. A terrorist is a person who uses unlawful violence and intimidation, especially against civilians, in the pursuit of political aims. Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transhipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Sanctions	Sanctions are restrictive measures imposed by CAs against natural persons (individuals), groups (are inclusive of terrorist groups, religious groups, financial groups, etc.), legal persons / entities and / or countries to prevent and suppress terrorism and terrorist financing.
Prominent Influential Persons	PIP/PEPs are individuals who are or have been entrusted with prominent public functions, including heads of state or of government, senior politicians, senior

Term	Description
(Politically Exposed Persons) (PIP/PEP)	government, judicial or military officials, senior executives of publicly owned corporations and important political party officials.