PREVENTION OF MONEY LAUNDERING AND THE COMBATTING OF THE FINANCING OF TERRORISM POLICY

CONTENTS

1. PURPOSE OF THE POLICY

This document defines the Prevention of Money Laundering and the Combating of the Financing of Terrorism Policy for Hollard Holdings ("Hollard") and the regulated entities operating within the Group.

Money Laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

Terrorism Financing refers to activities which involves the solicitation, collection and the providing of funds and other assets with the intention that it may be used to support terrorist acts, terrorist organisations or individual terrorists.

Managing money laundering risks requires robust controls that must also be implemented to manage any risks associated with the financing of terrorism.

The purpose of this policy is to outline the minimum standards of internal Anti Money Laundering ("AML") controls and Counter Terrorism Financing ("CTF") controls that must be applied by Hollard in order to mitigate the legal, regulatory, reputational and subsequent financial risks.

2. APPLICATION OF THIS POLICY

The requirements set out in this policy apply to Hollard and define the responsibilities and accountabilities for the Group.

The implementation of this policy will be proportionate to the nature, scale and complexity of each of the various Companies. The principle of proportionality is of particular importance to ensure the consistent application of the policy whilst ensuring a fair and balanced approach to implementation. Proportionality is broadly defined with reference to the following measures:

- *Nature* – The specific nature of Hollard's activities including, for example, types of lines of business and the number of lines of business;

- *Scale* – The size of Hollard's business activities including for example gross premium and maximum risk retention;

- *Complexity* – The complexity of Hollard's business and its activities including the business and distribution model, governance structures, product design, number of lines of business and special or alternative risk transfer activities.

This Policy applies to all Hollard employees, contractors, partners, vendors, intermediaries and non-compliance to the policy may lead to disciplinary, regulatory, criminal and civil proceedings. The Hollard Group Compliance Regulatory Non-Compliance process must follow when there has been an infringement of FICA or Hollard's Prevention of Money Laundering and the Combatting of the Financing of Terrorism Policy.

The implementation, accountabilities, roles and responsibilities in terms of this policy will be applied in terms of the three lines of defence as outlined in the Enterprise Risk Management (ERM) Framework.

3. LEGAL AND COMPLIANCE APPETITE STATEMENT

Hollard is committed to avoid the risk of non-compliance to regulatory obligations. The Hollard Board and Senior Management is committed to conducting the business affairs of Hollard in an ethically and legally compliant manner with due regard of our responsibilities towards our customers, shareholders, regulators and the environment in which we operate.

Hollard will not knowingly engage in any transaction, product development or initiative or design or implement any procedure or control that will result in a non-compliance.

4. POLICY FORMULATION

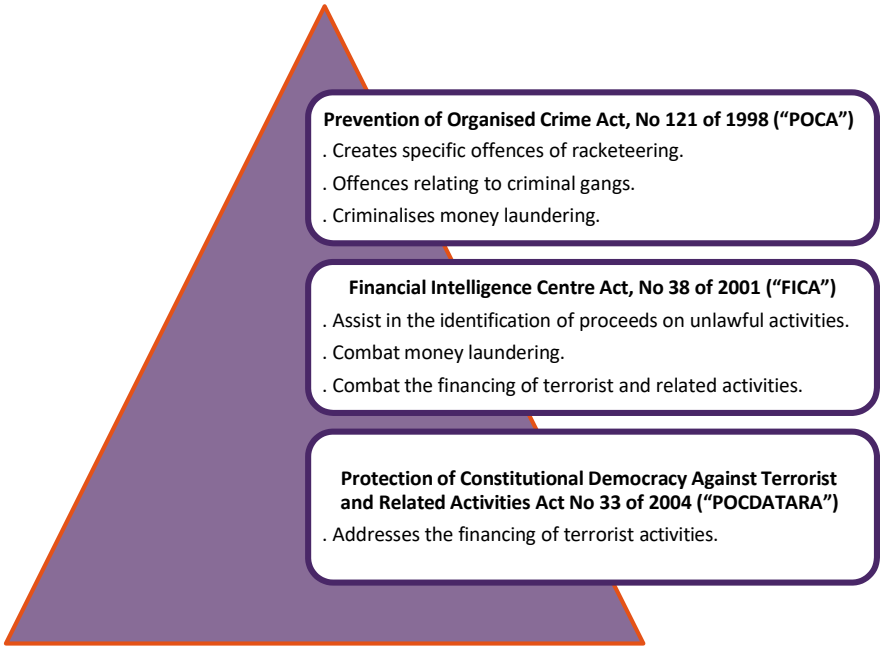
The principles and objectives of the Hollard Prevention of Money Laundering and the Combatting of the Financing of Terrorism Policy will be supported by several policies, standards, procedures and other documentation adopted throughout Hollard, as well as relevant regulatory and compliance frameworks.

5. ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING LEGAL AND REGULATORY FRAMEWORK

The Financial Action Task Force (“FATF”), an independent inter-governmental body develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

The FATF Recommendations are taken into account in South Africa in developing a comprehensive framework or measures to combat money laundering and terrorist financing as well as the financing of proliferation of weapons of mass destruction.

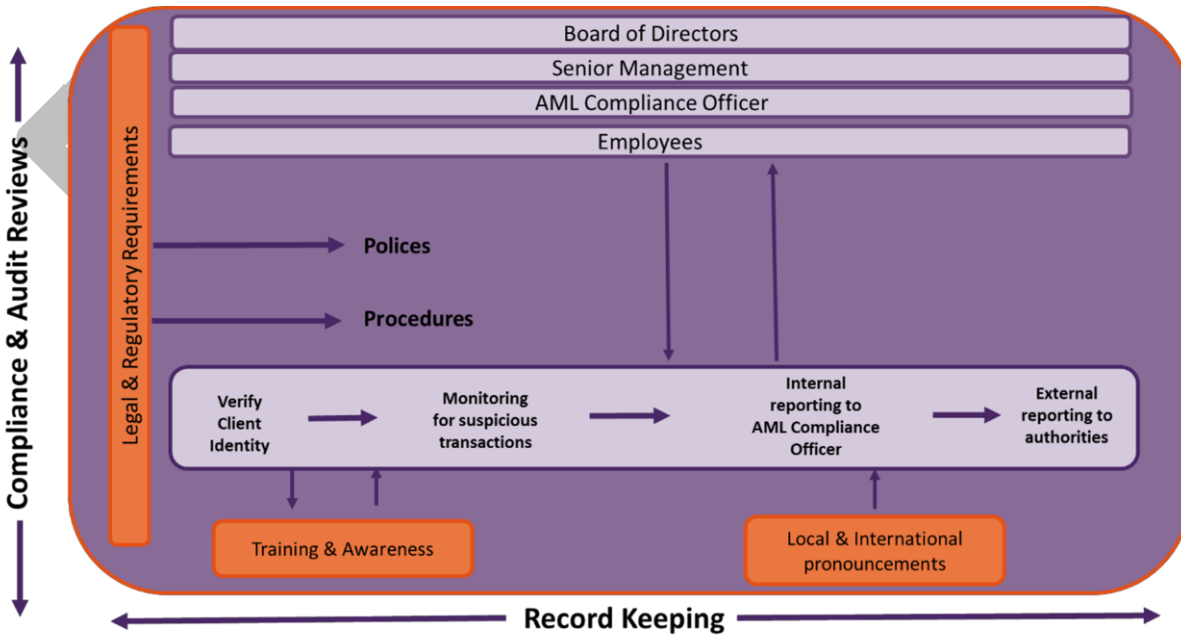
The following legal and regulatory framework is applicable in South Africa:



6. ANTI MONEY LAUNDERING AND COUNTER TERRORISM FINANCING OPERATING MODEL

Hollard has in place an operating model that is supportive of a culture of compliance. The operating model is explicit in the Hollard Compliance Policy.

Hollard has implemented a clear operating model for managing money laundering risks and the combatting of terrorist financing risks. The operating model is represented in the diagram below:



7. ROLES AND RESPONSIBILITIES

The Board delegates certain operational responsibilities as set out below but remains ultimately accountable and will oversee the performance of the delegated responsibilities.

a) **The Hollard Group Board is responsible to:**

- Ensure that the organisation has the required structures in place to manage money laundering risks and to counter terrorism financing risks; and
- Approve policies to mitigate the risks of money laundering and terrorist financing to minimise the impacts thereof.

b) **Hollard Senior Management is responsible to:**

- Implement policies and procedures to manage money laundering risks and terrorism financing risks;
- Develop processes that identify, manage and monitor money laundering risks and terrorism financing risks that may be incurred by the organisation;
- Monitor the appropriateness, adequacy and effectiveness of the anti-money laundering and counter terrorism financing risk management system;
- Responsible for ensuring that employees adhere to policies and procedures to prevent money laundering and terrorist financing risks;
- Undertake a risk assessment which identifies the vulnerability of the organisation to be used to launder money or finance terrorists;
- Implement risk management controls to ensure that the organisation is not used to launder money or finance terrorists;
- Ensure the risk management procedures are risk-based with sufficient resources being devoted to dealing with higher-risk customers and transactions;
- Devote sufficient resources to deal with money laundering and terrorist financing and ensure employees receive appropriate and adequate training;
- Conduct anti-money laundering and counter terrorism financing risk assessment and implement a Risk Management Compliance Programme (“RMCP”), aligned to this policy;
- Consult with the AML Compliance Officer in developing a Business Unit specific anti-money laundering and counter terrorism financing compliance monitoring plan that at a minimum addresses key anti-money laundering and counter terrorism financing compliance risks;
- Report monitoring results and any other significant internally identified anti-money laundering and counter terrorism financing compliance matters to the AML Compliance Officer;
- Facilitate the immediate reporting of actual or potential money laundering and terrorist financing risks to the responsible persons in business and inform the AML Compliance Officer and the Financial Intelligence Centre (“FIC”) and provide guidance to the employees on the reporting of suspicious transactions;
- Ensure business systems are developed to manage new accounts and a customer verification process is in place for customer due diligence;

- Facilitate the collation of any data or information requested by the AML Compliance Officer; and
- Assist the AML Compliance Officer in the execution of their responsibilities by complying with requests for information or assistance in a timely manner.

c) **Hollard AML Compliance Officer is responsible to:**

- Develop and maintain the prevention of money laundering and the combatting of the financing of terrorism policy and internal procedures of the organisation in line with legislative requirements;
- Assist Senior Management in developing and maintaining an effective anti-money laundering and counter-terrorist financing compliance culture;
- Ensure the organisation's risk management policies regarding prevention of money laundering and terrorist financing, risk assessments, and their application are adequately documented;
- Ensure Senior Management adopt a risk-based approach regarding money laundering and terrorist financing and conduct a risk assessment of the organisation's customers, products, services, delivery channels, and geographic reach;
- Ensure all internal suspicious activity reports and trends relating to money laundering and terrorist financing are investigated without delay;
- Ensure that suspicious transaction reports and other legislative reports are timeously submitted to Financial Intelligence Centre ("FIC");
- Ensure money laundering and terrorist financing awareness training is delivered to the Board, Senior Management and employees;
- Ensure employees are aware of and complying with their obligations of the legislation, policies and procedures and the basis for the risk-based approach to managing money laundering and terrorist financing risks is understood and applied;
- Present reports to the Board, Sub-Committees, and Senior Management; making recommendations, if any, for action to remedy any deficiencies in the policies, procedures, systems, or controls and following up on those recommendations;
- Represent the organisation at all external agencies, supervisory, regulatory, or law enforcement agencies;
- Ensure a review process is in place for all alerts regarding all incoming and outgoing payments and taking the necessary decisions on reported matches and false positives in relation to money laundering or terrorist financing;
- Awareness of any relevant sanctions and prohibition or advisory notices issued by the supervisory agency, FIC, or other agencies such as the United Nations Security Council;
- Respond promptly to any reasonable request for information from the supervisory, regulatory, and / or law enforcement agencies;
- Ensure the required screening of all new accounts, relationship updates, and ongoing updates of enhanced due diligence and risk assessment reports are carried out in accordance with the requirements set out in this policy; and
- Ensure an automated list of all high-risk customers is produced.

d) **Hollard Employees are responsible to:**

- Carry out their responsibilities according to the policy and procedures developed to manage money laundering and terrorist financing risks;
- Ensure no transactional activity is undertaken without a clear understanding of the purpose and background of the transaction(s) or activity(ies);
- Report promptly to the BU Compliance team and/ or Money Laundering Reporting Officer ("MLRO") when they have knowledge or suspicion of money laundering or the financing of terrorism or where there are reasonable grounds to know of or suspect money laundering or terrorist financing;
- Not tip off any customer or any person that a suspicious transaction report has been made or that their account and / or transactions are under investigation either internally by the Assurance functions or externally by the FIC;
- Assist / support Senior Management, MLRO or the AML Compliance Officer with any reported matters; and
- Complete a record of when they have received anti-money laundering and counter terrorism financing training and the nature of that training.

e) **Hollard Internal Audit and Group Compliance is responsible to:**

- Conduct an independent review of the organisation's anti-money laundering and counter terrorism financing program, at least once every year. The review should be performed in accordance with the established audit and compliance procedures, including review of samples of transactions and of account opening documentation.

  The review of the compliance program should cover the following:
  - Customer identification and verification;
  - Suspicious transaction reporting including other reporting requirements under FICA, record keeping, and retention;
  - The role and responsibilities of the AML Compliance Officer; and
  - Ongoing employee training.

  Results of the reviews should be reported to the identified Committee, including recommendations to rectify deficiencies identified.

8. RISK BASED APPROACH (RBA) AND RISK MANAGEMENT COMPLIANCE PROGRAMME (RMCP)

The RBA takes the following steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by Hollard:

- Identify and assess the money laundering and terrorist financing risks that are relevant to Hollard;
- Design and implement controls to manage and mitigate the assessed risks; and
- Monitor and improve the effective operation of these controls.

Risk management generally shall be regarded as a continuous process, carried out on a dynamic basis. Hollard's governance structures therefore must ensure that their risk management

processes for managing money laundering and terrorist financing risks are kept under regular review. The RBA principles are required to consider the identification, assessment, understanding and mitigation of money laundering and terrorist financing risk including explicit consideration to key risk factors such as geography, customer, product and delivery channel and with varying degrees of impact and levels of risk. Where Hollard identifies higher risks, Hollard must ensure that anti-money laundering and counter terrorism financing procedures adequately addresses such risks. Where Hollard identifies lower risks, Hollard may decide to implement simplified measures under certain conditions within the provisions of the relevant legislation

The RMCP must be implemented to set out the manner in which and process by which the establishment and verification of clients will be undertaken.

9. CUSTOMER DUE DILIGENCE ("CDD")

Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development of an overall risk framework.

Effective CDD processes must include the following:

- Quick, Standard or enhanced identification and verification requirements for all customers;
- Enhanced due diligence (obtaining additional information on the customer, obtaining information on the source of funds or wealth of the customer, conducting enhanced monitoring of the business relationship) for higher-risk customers, as determined by the risk assessment;
- Where appropriate, reduced CDD requirements where the risk of money laundering or terrorist financing has been assessed as being low;
- Ongoing risk-based monitoring of customer activities and transactions that will enable the organisation to ensure transactions being conducted are consistent with the organisation's knowledge of the customer. Customers assessed to be a higher risk will be subject to enhanced monitoring compared with customers assessed to be a low risk; and
- In addition, background information must be collected on high-risk customers; Domestic Prominent Influential Persons ("DPIPs), Foreign Prominent Influential Person ("FPIPs"), Foreign Prominent Public Official ("FPPOs") or family members and known associates of domestic and foreign influential persons; individuals deemed high risk, geographically or otherwise; and companies and/or institutions that trade in or do business related to high-risk commodities. This will also involve obtaining information to substantiate the source of wealth and funds of a high-risk customer.

10. REPORTING

Reports of suspected money laundering and terrorist financing risks must be reported the Business Unit Assurance functions, BU Compliance teams and/ or MLRO's, who will be responsible for reporting to the FIC. Reports may also be made via email (fraud@hollard.co.za) or by reporting via the external hotline (0801-516-170 or Hollard@tip-offs.com).

11. RECORD KEEPING

All records are kept for at least five-years after the termination of a business relationship and contain records obtained through CDD measures; account files and business correspondence; the results of any analysis undertaken; documents relating to business relations and executed transactions; correspondence with the clients and other persons with whom Hollard keeps a business relation.

12. TRAINING

Hollard shall take measures proportionate to their risks, nature and size so that their employees are aware of the provisions adopted pursuant to managing money laundering and terrorist financing risks, including relevant data protection requirements. Those measures shall include participation of their employees in special ongoing training programs to help them recognise operations which may be related to money laundering and terrorist financing and to instruct them how to proceed in such cases. Hollard shall refresh employees' knowledge on the practices of money laundering and terrorist financing and on indications leading to the recognition of suspicious transactions.

13. POLICY ADMINISTRATION

Anti- Money Laundering Compliance Officer (AMLCO): Wikus Luus

Version Control:

Policy Name	Version	Approval Date
Prevention of Money Laundering and the Combatting of the Financing of Terrorism Policy	2	December 2019

Frequency of Review	Date of Next Review	Date of Last Review
Every two years or as required	December 2021	December 2019