

## AML POLICY

### Maono Global Markets (Pty) Ltd

#### CONTENTS..... Error! Bookmark not defined.

1. DEFINITIONS AND INTERPRETATION .....	1
2. DISCLAIMER:.....	8
3. POLICY STATEMENT: .....	8
4. RISK ASSESSMENT: .....	9
5. CUSTOMER DUE DILIGENCE (CDD):.....	9
6. ENHANCED DUE DILIGENCE (EDD):.....	10
7. SUSPICIOUS ACTIVITY REPORTING (SAR): .....	11
8. RECORD KEEPING: .....	11
9. EMPLOYEE TRAINING: .....	12
10. COMPLIANCE MONITORING: .....	13
11. REPORTING AND ESCALATION: .....	14
12. REGULATORY COMPLIANCE: .....	15

## 1. DEFINITIONS AND INTERPRETATION

### 1.1. Definitions

For the purposes of this AML Policy (“Policy”), the following terms shall have the meanings set out below. Unless the context indicates otherwise, words importing any gender include all genders, words importing the singular include the plural and vice versa, and references to “including” or “includes” are deemed to be without limitation.

**1.1.1. “Account”** means any trading, transactional or client account opened or maintained with Maono Global Markets (Pty) Ltd through which a Client is able to access and use the trading platform and related services.

1.1.2. **“Administrative Sanctions”** means any sanctions, penalties, administrative fines, remedial directions or restrictive measures imposed by a Supervisory Authority or other competent authority for non-compliance with Applicable AML Laws.

1.1.3. **“AML” or “Anti-Money Laundering”** means all measures, policies, procedures, controls and activities designed to prevent, detect, mitigate, report and remediate Money Laundering and related financial crimes, including Terrorist Financing and Proliferation Financing.

1.1.4. **“Applicable AML Laws”** means all applicable laws, regulations, rules, directives, guidance notes and regulatory instruments relating to anti-money laundering, counter-terrorist financing and counter-proliferation financing in force in the Republic of South Africa from time to time, including without limitation:

- 1.1.4.1. The Financial Intelligence Centre Act, 38 of 2001 (“FICA”) and regulations made under it;
- 1.1.4.2. The Prevention of Organised Crime Act, 121 of 1998 (“POCA”);
- 1.1.4.3. The Protection of Constitutional Democracy Against Terrorist and Related Activities Act, 33 of 2004 (“POCDATARA”);
- 1.1.4.4. The Financial Sector Regulation Act, 9 of 2017 (“FSR Act”); and

1.1.4.5. any directives, guidance notes, public compliance communications and rulings issued by the **Financial Intelligence Centre (“FIC”)**, the **Financial Sector Conduct Authority (“FSCA”)**, and any other competent authority, as amended or re-enacted from time to time.

1.1.5. **“Beneficial Owner”** means the natural person(s) who ultimately owns or effectively controls a Client or on whose behalf a transaction is being conducted, including, without limitation:

- 1.1.5.1. in relation to a legal person other than a listed company, the natural person(s) who directly or indirectly owns or controls 25% or more of the shares, voting rights or ownership interest in that legal person, or who otherwise exercises effective control over the management or policies of that legal person;
- 1.1.5.2. in relation to a partnership, the natural person(s) who ultimately are entitled to or control 25% or more of the partnership’s capital or profits, or who otherwise exercise effective control over the partnership; and

1.1.5.3. in relation to a trust, the founder, the trustees and the beneficiaries, as well as any other natural person who exercises ultimate effective control over the trust.

1.1.6. **“Business Day”** means any day other than a Saturday, Sunday or official public holiday in the Republic of South Africa on which banks are generally open for business.

1.1.7. **“Client” or “Customer”** means any natural or legal person who applies for, is on-boarded for, or makes use of the trading platform, products or services made available through Maono Global Markets (Pty) Ltd as juristic representative of Sithundhi Group (Pty) Ltd, including any prospective client during the on-boarding process.

1.1.8. **“Client Agreement”** means the legally binding client agreement (including terms and conditions, policies and schedules) concluded between the Client and RocketX (Pty) Ltd, which governs the use of the trading platform and the provision of derivative products and services.

1.1.9. **“Compliance Function”** means the person(s) and function(s) responsible for overseeing and coordinating compliance with Applicable AML Laws and this Policy, including the appointed Money Laundering Reporting Officer (MLRO) and his/her delegates.

1.1.10. **“Counterparty”** means RocketX (Pty) Ltd, in its capacity as principal and contractual counterparty to Clients in relation to the derivative contracts traded via the platform.

1.1.11. **“Customer Due Diligence” or “CDD”** means the identification and verification measures, information-gathering and risk assessment processes undertaken in respect of a Client, including but not limited to:

- 1.1.11.1. identifying and verifying the Client’s identity;
- 1.1.11.2. identifying and verifying the Beneficial Owner(s), where applicable;
- 1.1.11.3. understanding the nature and intended purpose of the business relationship; and
- 1.1.11.4. conducting ongoing monitoring of the business relationship and transactions, as required by Applicable AML Laws and this Policy.

1.1.12. **“Enhanced Due Diligence” or “EDD”** means additional or more intensive due diligence measures applied to higher-risk Clients, products, services, jurisdictions or transactions, beyond standard CDD measures, including (without limitation) obtaining additional information on the Client or Beneficial Owner, the source of funds, source of wealth, and enhanced ongoing monitoring.

1.1.13. **“FIC”** or **“Financial Intelligence Centre”** means the Financial Intelligence Centre established in terms of section 2 of FICA, or any successor body.

1.1.14. **“FSCA”** means the Financial Sector Conduct Authority established in terms of the FSR Act, or any successor body.

1.1.15. **“High-Risk Country”** or **“High-Risk Jurisdiction”** means any country or jurisdiction that is:

- 1.1.15.1. identified by the FIC, FSCA or any other South African regulatory authority as presenting a high risk of Money Laundering, Terrorist Financing or Proliferation Financing;
- 1.1.15.2. identified by the Financial Action Task Force (FATF) as a high-risk jurisdiction subject to a call for action or increased monitoring; or
- 1.1.15.3. otherwise assessed by Maono Global Markets (Pty) Ltd, in its risk assessment, as presenting an elevated AML risk.

1.1.16. **“High-Risk Client”** means a Client that Maono Global Markets (Pty) Ltd has assessed as posing a higher than normal risk of Money Laundering, Terrorist Financing or Proliferation Financing, having regard to the risk factors set out in this Policy, the risk assessment methodology and Applicable AML Laws.

1.1.17. **“Jurisdiction”** means any country, territory or region in which Maono Global Markets (Pty) Ltd or RocketX (Pty) Ltd offers or makes available its products or services, or in which Clients are located or resident.

1.1.18. **“Juristic Representative”** means Maono Global Markets (Pty) Ltd, appointed and authorised as a juristic representative of Sithundhi Group (Pty) Ltd in terms of the Financial Advisory and Intermediary Services Act, 37 of 2002 (“FAIS Act”), and reflected as such on the FSCA’s register of authorised financial services providers.

1.1.19. **“KYC”** or **“Know Your Customer”** means the processes of identifying and verifying the identity of Clients, understanding the nature of their activities and assessing their AML risk, as required for CDD and EDD under this Policy and Applicable AML Laws.

1.1.20. **“Material AML Breach”** means any material failure to comply with this Policy or Applicable AML Laws which may reasonably be expected to expose Maono Global Markets (Pty) Ltd, Sithundhi Group (Pty) Ltd or RocketX (Pty) Ltd to regulatory sanction, criminal liability, reputational damage or material financial loss.

1.1.21. **“MLRO” or “Money Laundering Reporting Officer”** means the individual appointed by Maono Global Markets (Pty) Ltd (and/or by Sithundhi Group (Pty) Ltd, as applicable) in terms of FICA as the person responsible for receiving internal reports of suspicious or unusual transactions, considering such reports and, where appropriate, filing reports with the FIC and other competent authorities.

1.1.22. **“Money Laundering”** means any act or attempted act to conceal or disguise the nature, source, location, disposition or movement of the proceeds of unlawful activities, or any interest in such proceeds, as contemplated in POCA and any similar or related offences in Applicable AML Laws, and includes, without limitation:

1.1.22.1. the conversion or transfer of property, knowing that such property is the proceeds of unlawful activities, for the purpose of concealing or disguising the illicit origin of the property;

1.1.22.2. the concealment or disguise of the true nature, source, location, disposition, movement or ownership of, or rights with respect to, property, knowing that such property is the proceeds of unlawful activities; or

1.1.22.3. the acquisition, possession, use or dealing with property, knowing or having reasonable grounds to suspect that such property is the proceeds of unlawful activities.

1.1.23. **“Ongoing Monitoring”** means the continuous or periodic review of the business relationship and transactions undertaken by or on behalf of a Client to ensure that they are consistent with the institution’s knowledge of the Client, its business and risk profile, including, where necessary, the source of funds, and to identify any suspicious or unusual activity.

1.1.24. **“PEP” or “Politically Exposed Person”** means a natural person who is, or has been, entrusted with prominent public functions, whether domestically or in a foreign jurisdiction, and includes, without limitation, heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state-

owned corporations, important political party officials, as well as their immediate family members and close associates, as further described in FICA and applicable guidance.

1.1.25. **“Proliferation Financing”** means the provision or collection of funds or the making available of economic resources, directly or indirectly, and by any means, with the intention that they should be used or in the knowledge that they are to be used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery, and related materials.

1.1.26. **“Risk Assessment”** means the process described in this Policy whereby Maono Global Markets (Pty) Ltd identifies, assesses and understands its Money Laundering, Terrorist Financing and Proliferation Financing risks at enterprise, product, service, jurisdiction, delivery channel and Client levels, and implements risk mitigation measures and controls.

1.1.27. **“RocketX (Pty) Ltd”** means RocketX (Pty) Ltd (registration number 2020/824856/07), a licensed Financial Services Provider and Over the Counter Derivatives Provider, which issues the derivatives traded by Clients through the platform and acts as principal and counterparty to those transactions.

1.1.28. **“Sanctions”** means any economic, financial or trade sanctions, embargoes, restrictive measures or similar actions imposed by the Republic of South Africa, the United Nations Security Council, or any other sanctions authority recognised by Maono Global Markets (Pty) Ltd, and which are applicable to the business or its Clients.

1.1.29. **“SAR” or “Suspicious Activity Report”** means any report made to the FIC or other competent authority, in accordance with Applicable AML Laws, regarding a transaction or activity that is known or suspected to involve proceeds of unlawful activities, Money Laundering, Terrorist Financing, Proliferation Financing or other reportable conduct.

1.1.30. **“Sithundhi Group (Pty) Ltd”** means Sithundhi Group (Pty) Ltd (registration number 2021/817017/07), an authorised financial services provider with FSP No. 52030, as reflected in the Disclaimer section of this Policy, and the principal under which Maono Global Markets (Pty) Ltd acts as Juristic Representative.

1.1.31. **“Terrorist Financing”** means the provision, collection or making available of funds or other assets, by any means, directly or indirectly, with the intention that they be used,

or in the knowledge that they are to be used, in full or in part, to carry out any act of terrorism or terrorist-related activity as contemplated in POCDATARA or other Applicable AML Laws.

- 1.1.32. **“Trading Platform”** means the online trading system, portal, website, mobile application or other electronic facility provided to Clients by Maono Global Markets (Pty) Ltd (as Juristic Representative) and/or by RocketX (Pty) Ltd, through which Clients may access the derivative products and services.
- 1.1.33. **“Transaction”** means any payment, deposit, withdrawal, transfer, trade, order, contract for difference, derivative transaction, or other movement of funds or assets executed or attempted by, on behalf of, or for the benefit of a Client via the Trading Platform or any linked payment or settlement channels.
- 1.1.34. **“Unusual Transaction”** means any transaction which is inconsistent with the known legitimate business or personal activities, risk profile, source of funds or transactional history of the Client, or which otherwise lacks an apparent lawful or economic purpose, having regard to the applicable context and guidance issued by the FIC.
- 1.1.35. **“Whistle-blower”** means any employee, contractor or other person who, in good faith, reports a suspected breach of this Policy, a suspected AML/CTF concern, or any suspicious or unusual transaction through the reporting channels described in this Policy.

## 1.2. Interpretation

- 1.2.1. References to **“Maono Global Markets (Pty) Ltd”** or **“Maono”** in this Policy include its directors, officers, employees and authorised representatives, acting within the course and scope of their duties, unless the context indicates otherwise.
- 1.2.2. References to **“we”**, **“us”** or **“our”** in this Policy are references to Maono Global Markets (Pty) Ltd in its capacity as an authorised Juristic Representative of Sithundhi Group (Pty) Ltd, and, where appropriate, include Sithundhi Group (Pty) Ltd and RocketX (Pty) Ltd in relation to their respective AML roles and responsibilities.
- 1.2.3. Headings and sub-headings are for convenience only and shall not affect the interpretation of this Policy.

- 1.2.4. Any reference to a statute, regulation or other law is a reference to that law as amended, re-enacted or replaced from time to time, and includes all subordinate legislation, regulations, rules and directives made in terms thereof.
- 1.2.5. In the event of any conflict between this Policy and Applicable AML Laws, the provisions of Applicable AML Laws shall prevail to the extent of the inconsistency.
- 1.2.6. This Policy must be read together with the Client Agreement and any other internal policies and procedures forming part of the AML, compliance and risk management framework of Maono Global Markets (Pty) Ltd, Sithundhi Group (Pty) Ltd and RocketX (Pty) Ltd.

## 2. DISCLAIMER:

- 2.1. Maono Global Markets (Pty) Ltd with company registration number: 2023/599736/07 is an authorised Juristic Representative of Sithundhi Group (Pty) Ltd, South Africa, with company number: 2021/817017/07, an authorised financial services provider, licensed and regulated by the Financial Sector Conduct Authority (FSCA) of South Africa, with FSP No. 52030.
- 2.2. Maono Global Markets (Pty) Ltd, an authorised Juristic Representative of Sithundhi Group (Pty) Ltd, is the platform that Clients use to trade derivatives that are issued by RocketX (Pty) Ltd, registration number 2020/824856/07, a company registered under the laws of South Africa. RocketX (Pty) Ltd a licensed and regulated Financial Services Provider (FSP) and Over the Counter Derivatives Provider (ODP) with FSP Number: 52142 whose registered office is at Flexisuites, 141 Corobay Avenue, Menlyn, Gauteng 0181 is the counterparty and principal to the contract for difference purchased by you (the Client).
- 2.3. By using our services, you agree to be bound by the Client Agreement, which is entered into and binding between you (the Client) and RocketX (Pty) Ltd.

## 3. POLICY STATEMENT:

- 3.1. This Policy Statement serves as a comprehensive introduction, demonstrating our organisation's unwavering commitment to combating money laundering and adhering to the highest standards of Anti-Money Laundering (AML) laws and regulations.
- 3.2. We recognise the grave implications of money laundering and its detrimental effects on the integrity of financial systems, the economy, and society at large.

- 3.3. Our organisation firmly believes in upholding transparency, accountability, and ethical conduct in all financial transactions.
- 3.4. We are dedicated to implementing robust AML measures that not only protect our organisation but also contribute to the global effort in thwarting money laundering activities. By maintaining a strong and effective AML policy, we strive to safeguard our reputation, build trust with our customers, and uphold the integrity of the financial industry.
- 3.5. Our policy is built upon a foundation of continuous improvement, stringent risk assessment, diligent customer due diligence, comprehensive employee training, and robust reporting and compliance mechanisms.
- 3.6. Through these efforts, we aim to stay ahead of evolving AML risks, mitigate potential threats, and foster a culture of compliance that sets a standard of excellence in the fight against money laundering.

## 4. RISK ASSESSMENT:

- 4.1. Risk Assessment plays a pivotal role in our organisation's comprehensive Anti-Money Laundering (AML) program.
- 4.2. Through a meticulous evaluation process, we assess our exposure to money laundering risks, considering various factors that influence our risk profile. This includes a thorough analysis of our diverse customer base, the range of products and services we offer, the geographical locations in which we operate, and the specific risks associated with our industry. By identifying and understanding these risks, we can develop effective measures to mitigate them and implement tailored controls that align with our risk appetite.
- 4.3. Our risk assessment process is dynamic and proactive, ensuring that we stay abreast of emerging trends and evolving regulatory requirements.
- 4.4. We regularly review and update our risk assessment to adapt to changing circumstances, thus maintaining a robust AML framework that safeguards our organisation against money laundering threats and upholds the integrity of our operations.

## 5. CUSTOMER DUE DILIGENCE (CDD):

- 5.1. Customer Due Diligence (CDD) lies at the core of our Anti-Money Laundering (AML) efforts.

- 5.2. We have established robust procedures to diligently identify and verify the identity of our customers, whether they are individuals or legal entities, as well as to determine the beneficial owners.
- 5.3. Our CDD process involves comprehensive measures designed to minimise the risk of money laundering activities. This includes collecting and verifying relevant identification documents, conducting thorough risk-based assessments to understand the nature of the customer's activities, and implementing ongoing monitoring measures to detect any suspicious or unusual transactions.
- 5.4. By implementing rigorous CDD procedures, we ensure that we have a clear understanding of our customers' identities, business relationships, and the purpose of their transactions, enabling us to mitigate potential AML risks and maintain the integrity of our operations.

## 6. ENHANCED DUE DILIGENCE (EDD):

- 6.1. Enhanced Due Diligence (EDD) forms an integral part of our comprehensive Anti-Money Laundering (AML) program, enabling us to effectively manage higher-risk customers or transactions.
- 6.2. When dealing with individuals or entities classified as higher risk, such as politically exposed persons (PEPs) or customers from high-risk jurisdictions, we apply additional scrutiny through our EDD procedures.
- 6.3. These measures go beyond standard due diligence practices and involve gathering supplementary information to gain a more comprehensive understanding of the customer's profile and potential AML risks associated with their activities.
- 6.4. Our EDD process includes conducting enhanced background checks, performing more detailed risk assessments, and seeking additional documentation or independent verification.
- 6.5. By applying EDD measures, we strengthen our ability to identify and mitigate any potential money laundering risks, ensuring compliance with regulatory requirements, and maintaining the highest standards of integrity in our business relationships.

## 7. SUSPICIOUS ACTIVITY REPORTING (SAR):

- 7.1. Our organisation has implemented a robust framework for Suspicious Activity Reporting (SAR) as a vital component of our Anti-Money Laundering (AML) program.
- 7.2. This framework is designed to detect and report any suspicious transactions or activities that may raise concerns regarding potential money laundering or terrorist financing.
- 7.3. We have established clear guidelines and procedures to identify red flags, which are indicators of suspicious behaviour or transactions. These red flags encompass various factors, such as unusual transaction patterns, high-value transactions with no apparent legitimate purpose, inconsistent customer behaviour, or transactions involving high-risk jurisdictions or individuals.
- 7.4. When such red flags are identified, our dedicated team initiates a thorough investigation and, if necessary, files SARs with the appropriate regulatory authorities as per regulatory obligations.
- 7.5. Our commitment to SAR helps us contribute to the collective effort in combating financial crimes, maintaining the integrity of the financial system, and supporting law enforcement agencies in their efforts to disrupt illicit activities.

## 8. RECORD KEEPING:

- 8.1. At our organisation, we place great importance on maintaining accurate and up-to-date records as part of our Anti-Money Laundering (AML) program. We have implemented comprehensive policies to ensure the proper retention and management of customer information, transaction data, and AML-related documentation. These policies outline clear guidelines for the collection, storage, and protection of records in compliance with relevant laws and regulations.
- 8.2. We maintain a diligent record-keeping system that captures essential details such as customer identification documents, transactional information, risk assessment records, and any AML-related correspondence. These records are regularly updated to reflect any changes or updates to customer information or transactional data.
- 8.3. Our record-keeping policies also define appropriate retention periods for different types of records, ensuring compliance with legal and regulatory requirements. We retain records

for the duration specified by applicable laws and regulations, and in some cases, we may retain records for an extended period to meet our risk management or legal obligations.

- 8.4. We give utmost importance to data protection and confidentiality. Our record-keeping policies encompass measures to safeguard customer information and ensure secure access to records. We employ industry best practices and robust security protocols to protect against unauthorised access, loss, or misuse of records.
- 8.5. By maintaining accurate and well-organised records, we enhance our ability to conduct effective AML monitoring, risk assessments, and internal audits. These records serve as a reliable source of information for regulatory compliance purposes and assist in the investigation of any suspected financial crimes. Our commitment to sound record-keeping practices reinforces our dedication to upholding the highest standards of transparency, accountability, and compliance in our AML efforts.

## 9. EMPLOYEE TRAINING:

- 9.1. At our organisation, we prioritise employee training as a critical component of our Anti-Money Laundering (AML) program. We have developed comprehensive training programs designed to educate our employees about AML laws, regulations, and our organisation's specific policies and procedures.
- 9.2. Our training initiatives aim to raise awareness among staff members about the risks associated with money laundering and the importance of their roles in preventing such activities. Employees receive in-depth knowledge about the legal and regulatory framework governing AML, including the obligations and responsibilities imposed on our organisation.
- 9.3. The training programs cover various topics, such as recognising red flags and suspicious activities, conducting thorough customer due diligence, understanding the reporting requirements for suspicious transactions, and adhering to compliance procedures. We also provide guidance on the use of internal tools and systems designed to support AML efforts.
- 9.4. Our training is delivered through a combination of methods, including workshops, online modules, and informational materials. We regularly update our training programs to align with emerging trends, changes in laws and regulations, and industry best practices.

9.5. By ensuring that our employees are well-informed about AML regulations and equipped with the necessary knowledge and skills, we empower them to fulfil their roles effectively in detecting and preventing money laundering activities. This comprehensive training cultivates a culture of compliance and vigilance throughout our organisation, strengthening our collective efforts in safeguarding our operations and contributing to the broader global fight against financial crimes.

## 10. COMPLIANCE MONITORING:

10.1. Compliance monitoring is a crucial aspect of our Anti-Money Laundering (AML) program. We have established a systematic framework for ongoing monitoring and review to ensure the effectiveness of our AML efforts.

10.2. This framework includes regular internal audits and risk assessments that help us identify any potential gaps or deficiencies within our program. Internal audits play a vital role in assessing the implementation and adherence to our AML policies, procedures, and controls. Our dedicated audit team conducts independent and objective assessments to evaluate the effectiveness of our AML program.

10.3. These audits examine various areas, including customer due diligence practices, suspicious activity reporting, record-keeping, training programs, and overall compliance with applicable laws and regulations. The findings from these audits provide valuable insights into the strengths and weaknesses of our AML framework.

10.4. Risk assessments are another integral component of our compliance monitoring process. We conduct regular assessments to evaluate our exposure to money laundering risks, considering factors such as changes in our customer base, emerging industry risks, evolving regulatory requirements, and external factors that may impact our operations. Through these assessments, we identify and prioritise areas of higher risk, allowing us to allocate resources effectively and implement targeted risk mitigation measures.

10.5. By conducting regular compliance monitoring, including internal audits and risk assessments, we proactively identify any gaps or deficiencies in our AML program. This enables us to take timely remedial actions, make necessary improvements, and strengthen our controls. It also ensures that we remain in compliance with regulatory obligations and

industry best practices, upholding the integrity of our operations and reinforcing our commitment to combating money laundering effectively.

## 11. REPORTING AND ESCALATION:

- 11.1. Clear lines of communication and well-defined reporting channels are essential components of our Anti-Money Laundering (AML) program. We have established a robust framework that enables the timely reporting and escalation of AML-related issues to management or the designated compliance officer.
- 11.2. Within our organisation, we promote a culture of transparency and accountability, encouraging all employees to promptly report any AML concerns or suspicious activities they encounter. We have implemented a dedicated reporting mechanism, which includes designated points of contact and confidential channels for employees to raise AML-related issues.
- 11.3. When employees identify potential AML risks or suspicious transactions, they are encouraged to report them through the established reporting channels. These channels are designed to ensure the confidentiality and protection of the individuals reporting the concerns.
- 11.4. The reported AML-related issues are then escalated to the appropriate management or the designated compliance officer, who is responsible for overseeing the AML program. They have the necessary authority and expertise to review and evaluate the reported concerns, determine the appropriate course of action, and initiate any necessary investigations or follow-up measures.
- 11.5. We recognise the importance of timely and effective escalation in addressing AML risks and taking prompt action. By establishing clear reporting and escalation channels, we enhance our ability to respond swiftly to AML concerns, mitigate potential risks, and ensure compliance with regulatory requirements.
- 11.6. Furthermore, we emphasise the protection of whistle-blowers and non-retaliation against individuals who report AML-related issues in good faith. We have policies in place to safeguard employees who come forward with concerns, ensuring their anonymity and protecting them from any adverse actions. commitment to maintaining the highest standards of integrity, transparency, and compliance in our AML efforts.

## 12. REGULATORY COMPLIANCE:

- 12.1. At our organisation, we have a strong commitment to regulatory compliance and maintaining adherence to applicable Anti-Money Laundering (AML) laws and regulations. We recognise the importance of staying up to date with evolving regulatory requirements and ensuring compliance with supervisory authorities and relevant industry standards.
- 12.2. We actively monitor and assess changes in AML laws and regulations, both at the national and international levels. Our dedicated compliance team keeps a close eye on regulatory developments, industry guidance, and best practices to ensure that our AML program remains aligned with the latest requirements.
- 12.3. Our commitment to regulatory compliance is reflected in our approach to ongoing training and education. We provide regular training sessions and updates to our employees to ensure they are aware of their obligations and responsibilities under the prevailing AML laws and regulations. This empowers our staff to effectively implement AML controls and measures in their day-to-day activities.
- 12.4. Additionally, we conduct regular internal reviews and assessments to evaluate our compliance with AML regulations and industry standards. This includes internal audits, risk assessments, and periodic reviews of our policies, procedures, and controls. These evaluations help identify any areas of non-compliance or opportunities for improvement, allowing us to take proactive measures to enhance our AML program.
- 12.5. We actively engage with regulatory authorities during examinations or inspections, providing the necessary information and cooperating fully to demonstrate our commitment to compliance.
- 12.6. By maintaining a strong focus on regulatory compliance, we ensure that our AML program is robust, effective, and in line with the highest standards set by supervisory authorities and relevant industry bodies. Our commitment to compliance underscores our dedication to combating money laundering, protecting our organisation, and upholding the integrity of the financial system.