ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

VORTEX FX

VERSION 1.0

Contents

Version Control

VERSION	REVIEWER NAME	DATE	NEXT REVIEW	COMMENTS
1.0		June 2024		

1. Introduction

Vortex FX ("the Company"," Vortex", "We", "Us", "Our") is dedicated to implementing and establishing comprehensive anti-money laundering (AML) and counter-terrorist financing (CTF) procedures based on the latest legislation and regulations issued in the country where the Company operates.

Money laundering is the process of cycling large amounts of illegally obtained money (cash-based, electronic, or in other forms such as cryptocurrency) into legitimate enterprises, assets, and accounts to make it appear that the income was obtained legally and, therefore, provide more flexibility with the income ("clean money").

Money laundering can take many forms, and while sophisticated controls are in place in the banking and related sectors, criminals and their financial specialists are also developing increasingly complex methods for concealing illegal income and feeding it into businesses to realise legitimate income.

All businesses present attractive opportunities for criminals and their specialist financial cohorts to target due to the high-value assets and investment opportunities that can provide a legitimate ongoing income.

There is also the threat of income from money laundering being used to finance terrorist activities, with the root source of the funds coming from related actions.

This policy covers the controls that Vortex FX has in place to mitigate any perceived money laundering attempts and the methods that we use to train our staff and notify the authorities of suspicious activity so a further investigation can be undertaken.

Relevant Laws

1. **The Proceeds of Crime Act 2002 (amended in 2015)**
    - This Act provides the legal framework for confiscating and recovering the proceeds of crime, as well as the obligations of financial institutions to report suspicious activities.
2. **The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017**
    - These regulations implement the EU's Fourth Money Laundering Directive (4MLD) and Fifth Money Laundering Directive (5MLD) into UK law, setting out detailed requirements for customer due diligence, reporting, and record-keeping.
3. **The Terrorism Act 2000 (amended in 2006 and 2008)**
    - This Act establishes offences related to terrorist funding and sets out the responsibilities of financial institutions to report knowledge or suspicion of terrorist financing.
4. **The Financial Action Task Force (FATF) Recommendations**
    - As an international standard, the FATF Recommendations guide jurisdictions in implementing robust AML and CTF measures. Vortex FX adheres to these recommendations as part of its commitment to global best practices.

5. **The Anti-Money Laundering and Counter-Terrorism Financing Act 2020 (UK)**
    - This recent Act enhances the legal framework for combating money laundering and terrorist financing, introducing stricter penalties and enhanced regulatory oversight.

Commitment to Compliance: By the legal framework prescribed by the Acts above, Vortex FX is committed to maintaining a robust compliance program that includes the following key components:

1. **Internal Controls and Procedures**
    - **System of Internal Controls:** Establishing and maintaining a system of internal controls and procedures designed to ensure ongoing compliance with AML and CTF laws and regulations. This includes customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring of transactions.
    - **Policies and Procedures:** Developing comprehensive AML and CTF policies and procedures that are regularly reviewed and updated to reflect legislation and best practice changes.
2. **Independent Testing**
    - **Internal and External Audits:** Conduct regular independent testing for compliance through internal and/or external audits. These audits assess the effectiveness of the AML and CTF program and identify areas for improvement.
    - **Continuous Improvement:** Implementing audit recommendations to enhance the effectiveness of AML and CTF controls and ensure compliance with regulatory requirements.
3. **Training and Awareness**
    - **Personnel Training:** Providing ongoing training for all personnel on AML and CTF regulations, the identification of suspicious transactions, and the procedures for reporting such activities. This training ensures that employees are knowledgeable about their responsibilities and equipped to recognise and respond to potential money laundering and terrorist financing activities.
    - **Role-Specific Training:** Tailoring training programs to the specific roles and responsibilities of employees to ensure that they understand the risks and controls relevant to their functions.
4. **Designation of a Compliance Officer**
    - **Compliance Officer Appointment:** Designating an appropriate officer responsible for the continuous oversight and enforcement of compliance with the Acts. The Compliance Officer is tasked with ensuring that the Company's AML and CTF policies and procedures are effectively implemented and adhered to.
    - **Reporting and Accountability:** The Compliance Officer reports directly to senior management and the board of directors, providing regular updates on the AML and CTF program status and any significant issues or developments.

These AML and CTF procedures will take effect upon approval by the Company's director and shall remain in operation unless amended by the director's authority. Any procedure amendments will be communicated to all relevant personnel and integrated into the Company's compliance program.

1. Company Information

Vortex FX is committed to upholding the highest standards of integrity and transparency in all its operations. As a regulated financial services provider, Vortex FX adheres to strict legal and regulatory requirements to ensure the security and compliance of its services.

- **Trading Name:** Vortex FX operates under the trading name of Vortex FX LTD.
- **Incorporation:** Vortex FX LTD is incorporated under registered No. 2023-00517 IBC by the Registry of International Business: Companies, Partnerships & Trusts.
- **Registered Office:** The registered office of Vortex FX LTD is located at Pinnacle St. Lucia, Robin Kelton Building, Choc Bay, PO Box CP 5600, Castries, St. Lucia.

2. Business Operations

Vortex FX provides brokerage services in foreign exchange (Forex) and other financial instruments to a global clientele. The Company's services are designed to cater to both individual and institutional investors, offering a range of trading options.

2. Roles and Responsibilities

All staff are responsible for being alert to Money Laundering and bringing any concerns to the Nominated Officer.

The Nominated Officer will:

- Review (and, in some cases, instruct) AML Assessments.
- Be the point of contact for reporting.
- Report breaches or make queries through formal channels.

The directors and Senior Managers must:

- Identify, assess, and manage risks effectively in the business and how they may be exploited to launder money or finance terrorism.
- Use risk assessment tools and relevant resources to identify high-risk countries identified by the Financial Action Task Force, Foreign Commonwealth and Development Office, financial sanctions targets, and Money Laundering Advisory Notice.
- Appoint a nominated officer to report suspicious activity to the National Crime Agency.

- Devote adequate resources to address the risk of money laundering and terrorism through allocating budgets for formal training, ensuring adequate time and resources are prioritised concerning high-value transactions, and conducting suitable risk assessments of our clients.

3. Third-Party Tools Used for AML

Vortex FX employs various third-party tools to enhance its Anti-Money Laundering (AML) efforts. These tools provide essential customer due diligence, transaction monitoring, risk assessment, and reporting capabilities leveraging advanced technologies and specialised services; Vortex FX ensures robust compliance with AML regulations and effective detection and prevention of financial crime.

1. Customer Due Diligence (CDD) and Know Your Customer (KYC) Tools:

Refinitiv World-Check

World-Check is a comprehensive risk intelligence database that provides detailed information on individuals and entities identified as high-risk. This includes politically exposed persons (PEPs), sanctioned entities, and those linked to financial crime.

Vortex FX uses World-Check to screen new and existing customers against global watchlists and databases, ensuring compliance with regulatory requirements and identifying potential risks during the customer onboarding process.

Refinitiv's solutions are integrated into Vortex FX's KYC processes to verify customer identities, assess risk levels, and ensure compliance with international AML standards. The tool helps streamline onboarding by automating identity verification and background checks.

Jumio

Jumio’s AI-powered identity verification solutions authenticate government-issued ID documents and perform biometric verification, ensuring the authenticity of customer identities for Vortex FX.

Onfido

Onfido’s platform combines document verification with biometric analysis, preventing fraud and accurately verifying customer identities for Vortex FX.

2. Transaction Monitoring Tools

Actimize

Actimize is a leading provider of AML solutions, offering advanced analytics and machine-learning capabilities for real-time transaction monitoring.

Vortex FX uses Actimize to monitor transactions for suspicious activity continuously. The tool analyses transaction patterns, detects anomalies, and generates alerts for further investigation. Actimize helps ensure that all transactions are scrutinised for potential money laundering and terrorist financing activities.

ComplyAdvantage

ComplyAdvantage offers real-time transaction monitoring and risk assessment tools that Vortex FX uses to detect and prevent financial crimes. By leveraging advanced algorithms and a comprehensive risk database, ComplyAdvantage enables continuous monitoring and immediate identification of suspicious activities.

Automated alerts and detailed risk profiles facilitate swift investigation and compliance reporting, enhancing Vortex FX's ability to maintain robust AML and CTF standards.

3. Risk Assessment and Screening Tools

Trulioo

Trulioo is a global identity verification service that provides access to over 400 data sources in more than 100 countries.

Vortex FX uses Trulioo to verify customers' identities during the onboarding process. The tool provides real-time identity verification, ensuring accurate and complete customer information. Trulioo helps prevent identity fraud and supports compliance with KYC and AML regulations.

Kount

Kount provides AI-driven fraud prevention solutions that deliver real-time risk assessments and insights for Vortex FX. By analysing customer transactions, Kount helps identify and mitigate potential risks and fraudulent activities. The platform's advanced algorithms and comprehensive data sets enable Vortex FX to proactively address threats, ensuring secure and reliable financial operations.

6. Enhanced Due Diligence (EDD) Tools

Dow Jones Risk & Compliance

Dow Jones Risk & Compliance offers tools for conducting enhanced due diligence and managing compliance risks.

Vortex FX utilises Dow Jones Risk & Compliance to perform in-depth background checks on high-risk customers and entities. The tool provides detailed reports on potential risks, including adverse media coverage, sanctions, and legal proceedings. This information is critical for making informed decisions and ensuring thorough due diligence.

4. Risk Assessments

1. Current Risk Assessment and Mitigation

At Vortex FX, we employ a comprehensive risk assessment framework to identify and mitigate potential risks associated with money laundering and terrorist financing. This framework is designed to ensure compliance with international standards and regulatory requirements.

1.1. Risk Assessment Process

1. **Risk Identification**
   - Identify potential risk factors for customers, transactions, geographical locations, and products/services offered.
   - Utilise internal and external sources to gather information on emerging risks and typologies.
2. **Risk Evaluation**
   - Evaluate the identified risks based on their likelihood and potential impact on the organisation.
   - Use a risk scoring system to categorise risks as low, medium, or high.
3. **Risk Mitigation Strategies**
   - Develop and implement controls to mitigate identified risks.
   - Regularly review and update risk mitigation measures to ensure their effectiveness.

1.2. Key Risk Mitigation Measures

1. **Enhanced Customer Due Diligence (CDD)**
   - Perform enhanced due diligence on high-risk customers, including those from high-risk jurisdictions or involved in high-risk industries.
   - Obtain additional information on the customer's background, source of funds, and the nature of their business activities.
2. **Transaction Monitoring**
   - Implement automated systems to monitor transactions in real time.
   - Set thresholds for transaction values and volumes that trigger alerts for further investigation.
   - Analyse transaction patterns to identify unusual or suspicious activities.
3. **Know Your Customer (KYC) Procedures**
   - Ensure thorough verification of customer identity through reliable and independent sources.
   - Collect and verify information on the beneficial owners of legal entities.
   - Maintain updated customer profiles and perform periodic reviews to ensure information remains current.
4. **Segregation of Duties**

- Separate responsibilities within the organisation to prevent conflicts of interest and ensure checks and balances.
- Designate specific roles for customer onboarding, transaction monitoring, and compliance oversight.

5. **Staff Training and Awareness**
   - Regularly train employees on AML regulations, risk assessment procedures, and red flags for suspicious activities.
   - Foster a culture of compliance within the organisation by promoting awareness of AML policies and procedures.
6. **Independent Audits and Reviews**
   - Conduct regular audits of the AML program to assess its effectiveness and compliance with regulatory requirements.
   - Review audit findings and implement recommendations to address any identified weaknesses or gaps.

2. Examples of Risk Mitigation in Practice

2.1. Scenario 1: High-Risk Jurisdiction Client:

- A new client from a high-risk jurisdiction attempts to open an account and deposit a large sum of money. The compliance team performs enhanced due diligence, including verifying the client's identity, source of funds, and business activities. Transactions from this client are monitored more closely for any unusual patterns.

2.2. Scenario 2: Unusual Transaction Patterns:

- The automated transaction monitoring system detects a client making a series of high-value transactions that deviate from their normal activity. The compliance team investigates these transactions, seeking additional information from the client and, if necessary, reporting suspicious activity to the relevant authorities.

Continuous Improvement

Vortex FX is committed to continuously improving its risk assessment and mitigation framework. This involves staying informed about new and emerging risks, adopting best practices, and leveraging advanced technologies to enhance the effectiveness of our AML measures.

3. Criteria for Identifying High-Risk Customers

Identifying high-risk customers is a crucial component of Vortex FX's AML policy. Due to their increased potential for involvement in money laundering or terrorist financing activities, high-risk

customers require enhanced due diligence and closer monitoring. Vortex FX employs a robust set of criteria to identify these customers.

3.1. Criteria for Identifying High-Risk Customers

1. **Geographical Risk**
   - **High-Risk Jurisdictions:** Customers from countries identified as high-risk by the Financial Action Task Force (FATF) or other international bodies. These include countries with weak AML regulations, high levels of corruption, or known to be havens for illicit activities.
   - **Sanctioned Countries:** Customers from countries subject to international sanctions or embargoes.
2. **Customer Type**
   - **Politically Exposed Persons (PEPs):** Individuals who hold or have held prominent public positions, such as government officials, senior executives of state-owned enterprises, or high-ranking military officers, including their family members and close associates.
   - **Non-resident Customers:** Customers who are not residents of the country where Vortex FX operates, particularly those from offshore financial centres.
   - **Anonymous or Nominee Accounts:** Accounts opened under fictitious names or those that use nominees to obscure the account holder's true identity.
3. **Business and Industry Risk**
   - **High-Risk Industries:** Customers are involved in industries known for higher money laundering risks, such as gambling, casinos, money service businesses, real estate, precious metals and stones, and cryptocurrency trading.
   - **Cash-Intensive Businesses:** These are businesses that primarily deal in cash transactions, making it difficult to track the source and destination of funds.
4. **Transaction Patterns**
   - **Unusual Transaction Volumes:** Customers conducting transactions that are unusually large compared to their known financial profile or business activities.
   - **Complex Transaction Structures:** Transactions involving multiple intermediaries, jurisdictions, or accounts, which complicate the tracing of funds.
   - **Frequent Large Deposits or Withdrawals:** Repeated high-value transactions that do not align with the customer's known activities.
5. **Account Activity**
   - **Inconsistent Account Usage:** Account activities that deviate significantly from the customer's established pattern or expected behaviour.

- **Rapid Movement of Funds:** Funds moved quickly through the account, particularly if they are transferred to high-risk jurisdictions or third parties with no apparent legitimate purpose.

6. **Customer Behaviour**
   - **Reluctance to Provide Information:** Customers who are unwilling or hesitant to provide requested information or documentation during the KYC process.
   - **Use of Third Parties:** Customers use intermediaries or third parties to conduct transactions on their behalf without a clear, legitimate reason.
7. **Source of Funds**
   - **Unverified Source of Wealth:** Customers whose source of wealth or funds cannot be adequately verified or appears inconsistent with their profile.
   - **High-Risk Funding Sources:** Funds originating from high-risk areas, industries, or activities known for higher money laundering risks.

3.2. Enhanced Due Diligence for High-Risk Customers

For customers identified as high-risk based on the criteria above, Vortex FX applies enhanced due diligence measures, including:

- **Detailed Customer Information:** Collect more comprehensive information on the customer's identity, business activities, source of wealth, and financial background.
- **Increased Monitoring:** Conducting more frequent and detailed monitoring of the customer's transactions and account activities.
- **Senior Management Approval:** Requiring approval from senior management before establishing or continuing business relationships with high-risk customers.
- **Regular Review:** Periodically review the customer's profile and transactions to ensure ongoing compliance with AML requirements.

3.3. Examples of High-Risk Customers

- **Scenario 1:** A new customer from a high-risk jurisdiction deposits significant money and requests frequent international transfers. Enhanced due diligence is performed, including verifying the source of funds and the purpose of the transactions, and the account is subject to continuous monitoring.
- **Scenario 2:** An existing customer suddenly starts engaging in large, complex transactions that deviate from their normal activity. The compliance team investigates the changes in behaviour, seeks additional information, and monitors the account closely for any suspicious activities.

4. Additional Verification Triggers

To further strengthen our Anti-Money Laundering (AML) framework, Vortex FX has established specific triggers that prompt additional verification processes.

These triggers are designed to detect and prevent suspicious activities by scrutinising high-risk transactions and customer behaviours thoroughly.

4.1. Additional Verification Triggers

1. **High-Value Transactions**
   - **Deposit Thresholds:** Any single deposit or a series of deposits exceeding $10,000 triggers additional verification. This includes scrutinising the source of funds and ensuring compliance with regulatory requirements.
   - **Large Withdrawals:** Similar to deposits, withdrawals exceeding a set threshold, such as $10,000, prompt further investigation to ensure the funds are legitimate and the transaction is not part of a money laundering scheme.
2. **Unusual Transaction Patterns**
   - **Significant Deviations:** Transactions that significantly deviate from a customer's usual pattern, such as sudden increases in transaction volume or frequency, trigger a review to understand the reasons behind the changes.
   - **Multiple Transactions Just Below Threshold:** Multiple transactions that fall just below the reporting threshold, conducted within a short time frame, indicate potential structuring activities and trigger additional verification.
3. **International Transfers**
   - **High-Risk Jurisdictions:** Transfers to or from countries identified as high-risk by international bodies such as the Financial Action Task Force (FATF) prompt further due diligence to ensure the legitimacy of the transaction.
   - **Frequent Cross-Border Transactions:** Customers engaging in frequent international transfers, especially involving high-risk jurisdictions, are subject to enhanced scrutiny.
4. **Account Activity**
   - **Dormant Accounts:** Sudden activity in dormant accounts, especially involving large transactions, triggers a review to verify the source and purpose of the funds.
   - **New Accounts with High Activity:** New accounts showing high levels of activity immediately after opening are reviewed to ensure they are not being used for fraudulent purposes.
5. **Customer Behaviour**

- **Reluctance to Provide Information:** Customers who are hesitant or refuse to provide required information or documentation during the Know Your Customer (KYC) process trigger further investigation.
- **Third-Party Involvement:** Accounts with frequent use of third parties or intermediaries to conduct transactions prompt additional verification to understand the reasons behind such activities.

6. **Source of Funds and Wealth**
   - **Unusual Funding Sources:** Transactions funded from sources that are unusual or not consistent with the customer's profile, such as unexpectedly large sums from unknown sources, trigger further investigation.
   - **Inconsistent Wealth Declaration:** Discrepancies between the customer's declared source of wealth and observed transaction behaviour prompt additional due diligence.

4.2. Enhanced Verification Measures

When a trigger is activated, Vortex FX implements the following enhanced verification measures:

1. **Detailed Transaction Review**
   - **Transaction Analysis:** Conduct a detailed review of the transaction(s) in question, including the source of funds, destination, and the purpose of the transaction.
   - **Documentation Verification:** Request additional documentation to verify the legitimacy of the transaction, such as invoices, contracts, or bank statements.
2. **Customer Profile Update**
   - **Enhanced KYC:** Update the customer's profile with additional information gathered during the verification process. This includes verifying identification documents, sources of funds, and business activities.
   - **Risk Reassessment:** Reassess the customer's risk level based on the new information and update their risk profile accordingly.
3. **Increased Monitoring**
   - **Ongoing Monitoring:** Place the customer under increased monitoring for a specified period to detect any further suspicious activities.
   - **Transaction Limits:** Implement temporary transaction limits or require pre-approval for large transactions during the monitoring period.
4. **Reporting and Escalation**
   - **Suspicious Activity Report (SAR):** If the enhanced verification measures raise concerns, file a Suspicious Activity Report (SAR) with the relevant financial authorities.

- **Internal Escalation:** Escalate the case to senior management or the compliance committee for further review and decision-making.

4.3. Examples of Additional Verification Triggers

- **Scenario 1:** A customer deposits $12,000 in a single transaction. The compliance team initiates additional verification, requests documentation to verify the source of funds, and monitors the account for any further high-value transactions.
- **Scenario 2:** A dormant account suddenly becomes active with multiple transactions totalling $9,900 each. The compliance team investigates the transactions for potential structuring activities, requests additional information from the customer, and closely monitors the account.

5. Example of Risk Assessment in Practice

This area details few practical scenarios to illustrate how Vortex FX conducts a risk assessment and implements mitigation measures. These examples demonstrate the procedures and processes used to identify, assess, and address potential money laundering risks.

5.1. Example 1: High-Risk Jurisdiction Client

Scenario: A new client from a country identified as high-risk by the Financial Action Task Force (FATF) wants to open an account and deposit significant money.

Risk Assessment Process

1. **Initial Screening**
   - The client's information is screened against international watchlists and databases to identify any red flags or sanctions.
   - The client's country of origin is flagged as high-risk due to weak AML regulations and high levels of corruption.
2. **Enhanced Due Diligence (EDD)**
   - Collect detailed information about the client's identity, including passport, proof of address, and source of wealth.
   - Request documentation to verify the source of the funds, such as bank statements, business contracts, or proof of income.
3. **Risk Scoring**
   - Based on the collected information, the client is assigned a high-risk score due to the combination of their jurisdiction and the large deposit amount.
4. **Approval Process**

- The account opening and deposit require approval from senior management due to the high-risk score.
- The compliance team reviews all documentation and conducts a thorough background check.

Mitigation Measures

- **Increased Monitoring:** The client's transactions are monitored more closely and frequently to detect any unusual activity.
- **Transaction Limits:** Temporary transaction limits are set to manage the risk while the account is under review.
- **Ongoing Review:** The client's account and activity are reviewed periodically to ensure compliance with AML policies.

Outcome: The client's account is approved with conditions, including enhanced monitoring and regular reviews. Any suspicious activity detected during ongoing monitoring will be reported to the relevant authorities.

5.2. Example 2: Unusual Transaction Patterns

Scenario: An existing client, who typically makes small, regular deposits, suddenly begins making large, frequent deposits that deviate from their normal activity.

Risk Assessment Process:

1. **Transaction Monitoring Alert**
   - The automated transaction monitoring system flags the unusual deposit pattern for further investigation.
   - An alert is generated for the compliance team to review.
2. **Customer Profile Review:**
   - Review the client's historical transaction patterns and profile information to understand their typical behaviour.
   - Contact the client to inquire about the reasons for the sudden change in deposit amounts and frequency.
3. **Enhanced Due Diligence (EDD)**
   - Request additional information and documentation from the client to verify the source of the new funds.
   - Analyse the client's explanation and supporting documents to assess the legitimacy of the transactions.

- All capital deposited has to be withdrawn in the same method to the same accounts that the capital is withdrawn from.

4. **Risk Reassessment:**
   - Reevaluate the client's risk score based on the new information and determine if the changes in behaviour are justified.

Mitigation Measures

- **Temporary Hold:** Place a temporary hold on large deposits until the source of funds can be verified.
- **Enhanced Monitoring:** Increase the frequency and depth of transaction monitoring for the client's account.
- **Documentation Requirements:** Require ongoing submission of documentation for large deposits to maintain transparency.

Outcome: If the client provides satisfactory explanations and documentation, their risk score may be adjusted, and the account will continue to be monitored closely. If the client fails to provide adequate information, further actions such as filing a Suspicious Activity Report (SAR) or terminating the business relationship may be considered.

Example 3: Politically Exposed Person (PEP)

Scenario: A new client is identified as a Politically Exposed Person (PEP), holding a high-ranking government position in a foreign country.

Risk Assessment Process:

1. **Initial Screening**
   - The client's information is screened against PEP databases and watchlists to confirm their status.
   - The client is flagged as high-risk due to their position and potential exposure to corruption.
2. **Enhanced Due Diligence (EDD)**
   - Collect detailed information about the client's political role, country of service, and any known affiliations.
   - Request documentation to verify the source of funds and ensure they are not linked to corrupt activities.
3. **Risk Scoring:**
   - Assign a high-risk score to the client based on their PEP status and associated risks.
4. **Approval Process:**

- The account opening and any large transactions require approval from senior management.
- Conduct a thorough background check and verify all provided documentation.

Mitigation Measures

- **Enhanced Monitoring:** Implement continuous and enhanced monitoring of the client's transactions to detect any suspicious activity.
- **Regular Reviews:** Conduct regular reviews of the client's profile and transaction history to ensure compliance with AML policies.
- **Escalation Protocols:** Establish clear protocols for escalating any suspicious activities involving PEPs to senior management and relevant authorities.

Outcome: The client's account is approved with stringent monitoring and regular reviews. Any suspicious activity detected during monitoring will be escalated and reported promptly.

By implementing these detailed risk assessment procedures and mitigation measures, Vortex FX effectively manages potential risks associated with high-risk customers and transactions, ensuring compliance with AML regulations and maintaining the integrity of its financial services.

5. Customer Due Diligence (CDD)

1. Customer Identification Program (CIP)

The Customer Identification Program (CIP) is a fundamental component of Vortex FX's Anti-Money Laundering (AML) policy. The CIP is designed to ensure that Vortex FX knows the identity of its customers and verifies their identities before establishing a business relationship.

This helps prevent money laundering, terrorist financing, and other illicit activities.

1.1. Key Components of the CIP

1. **Customer Information Collection**
    - **Individual Customers:** For individual customers, Vortex FX collects the following information:
        - Full name
        - Date of birth
        - Residential address
        - Contact information (phone number, email address)
        - Nationality

    - Government-issued identification number (e.g., passport number, national ID number)
- **Legal Entities:** For legal entities (e.g., corporations, partnerships), Vortex FX collects the following information:
    - The full legal name of the entity
    - Type of entity (e.g., corporation, partnership)
    - Country of incorporation or registration
    - Registered address and principal place of business
    - Identification of key management personnel and beneficial owners
    - Articles of incorporation or other legal documentation

2. **Verification of Identity**
    - **Documentation:** Vortex FX requires customers to provide valid, government-issued identification documents. For individuals, acceptable documents include passports, national ID cards, and driver's licenses. For legal entities, acceptable documents include certificates of incorporation, business licenses, and legal documents showing the entity's structure and ownership.
    - **Proof of Address:** Customers must provide proof of address, such as utility bills, bank statements, or rental agreements, to verify their residential or business address.
    - **Electronic Verification:** Vortex FX may use electronic verification methods to cross-check the provided information against public databases and third-party verification services.
3. **Beneficial Ownership Identification**
    - For legal entities, Vortex FX identifies and verifies the beneficial owners, defined as individuals who ultimately own or control the entity. This includes:
        - Obtaining information on individuals who own 25% or more of the entity's equity.
        - Verifying the identity of beneficial owners using the same documentation and verification standards as for individual customers.
4. **Risk-Based Approach**
    - **Risk Assessment:** Vortex FX uses a risk-based approach to determine the level of due diligence required for each customer. High-risk customers, such as politically exposed persons (PEPs) and customers from high-risk jurisdictions, undergo enhanced due diligence.

- **Ongoing Monitoring:** Customer information is continuously monitored and updated to ensure it remains current. Changes in a customer's profile, such as changes in ownership or address, trigger a re-verification process.

5. **Record Keeping**

- **Retention Period:** Vortex FX maintains records of all customer identification information and verification documents for at least five years after the end of the business relationship.
- **Accessibility:** Records are stored securely and are accessible only to authorised personnel. They are made available to regulatory authorities upon request.

2. Procedures for Implementing CIP

1. **Account Opening Process**
    - **Information Collection:** During the account opening process, Vortex FX collects the required information from the customer.
    - **Documentation Submission:** Customers are required to submit identification and proof of address documents.
    - **Verification:** The collected information and documents are verified using manual checks and electronic verification methods.
2. **Enhanced Due Diligence (EDD)**
    - **High-Risk Customers:** For high-risk customers, additional information and documentation are collected. This includes detailed information on the source of funds, the purpose of the account, and the customer's business activities.
    - **Senior Management Approval:** High-risk customers and transactions require approval from senior management before the account can be opened or the transaction processed.
3. **Ongoing Due Diligence**
    - **Periodic Reviews:** Customer information is reviewed periodically to ensure it remains accurate and up-to-date. High-risk customers are subject to more frequent reviews.
    - **Transaction Monitoring:** Ongoing monitoring of transactions helps detect any unusual or suspicious activity. Transactions that do not align with the customer's profile trigger further investigation.

3. Examples of CIP Implementation

3.1. Scenario 1: Individual Customer

- An individual customer wishes to open a trading account with Vortex FX. The customer provides their passport a utility bill as proof of address, and completes the online registration form. Vortex FX verifies the provided information using both manual and electronic methods. Once verification is complete, the account is approved, and the customer can begin trading.

3.2. Scenario 2: Corporate Customer

- A corporate entity wishes to open an account. The entity provides its certificate of incorporation, a list of directors, and documents identifying the beneficial owners. Vortex FX verifies the entity's information, including the identities of the beneficial owners. The account is then approved, subject to ongoing monitoring and periodic reviews.

By implementing a comprehensive Customer Identification Program, Vortex FX ensures that it knows its customers and verifies their identities, thereby reducing the risk of money laundering and other financial crimes.

4. Ongoing Monitoring

Ongoing monitoring is a critical component of Vortex FX's Anti-Money Laundering (AML) policy. This process involves continuously reviewing and analysing customer transactions and activities to detect and prevent money laundering, terrorist financing, and other suspicious activities.

By maintaining a proactive approach, Vortex FX ensures compliance with regulatory requirements and safeguards the integrity of its financial services.

Key Components of Ongoing Monitoring

1. **Transaction Monitoring**
    - **Automated Monitoring Systems:** Vortex FX employs advanced automated systems to monitor transactions in real time. These systems are configured to detect patterns, anomalies, and red flags indicative of suspicious activity.
    - **Transaction Thresholds:** Specific thresholds are set for transaction values and volumes. Transactions exceeding these thresholds trigger alerts for further investigation.
    - **Pattern Analysis:** The monitoring systems analyse transaction patterns over time to identify unusual or inconsistent behaviours compared to the customer's historical activity.
2. **Customer Activity Reviews**
    - **Regular Reviews:** Customer accounts and transactions are reviewed regularly to ensure that activities align with the customer's known profile and the declared purpose of the account.
    - **High-Risk Customers:** High-risk customers, such as politically exposed persons (PEPs) and those from high-risk jurisdictions, undergo more frequent and detailed reviews.
    - **Ad Hoc Reviews:** Ad hoc reviews are conducted when unusual activity is detected or new information about a customer comes to light.
3. **Updating Customer Information**
    - **Periodic Information Updates:** Vortex FX periodically requests updated information from customers to ensure that their profiles remain current and accurate. This includes verifying contact details, addresses, and beneficial ownership for legal entities.
    - **Event-Driven Updates:** Updates are triggered by significant events, such as changes in ownership, large transactions, or unusual account activity.
4. **Enhanced Due Diligence (EDD) for High-Risk Activities**

- **In-Depth Investigations:** When high-risk activities or transactions are identified, enhanced due diligence measures are applied. This involves collecting additional information and documentation to verify the legitimacy of the activity.
- **Senior Management Involvement:** High-risk cases are escalated to senior management for review and approval before proceeding.

5. **Suspicious Activity Reporting (SAR)**
    - **Identification of Suspicious Activities:** Any transaction or activity that raises suspicion of money laundering or other illicit activities is flagged for further investigation.
    - **Filing SARs:** If an activity is deemed suspicious after investigation, a Suspicious Activity Report (SAR) is filed with the relevant financial authorities in compliance with regulatory requirements.
6. **Record Keeping**
    - **Documentation:** Detailed records of all monitoring activities, investigations, and findings are maintained. This includes records of alerts, reviews, and any actions taken.
    - **Retention Period:** Records are kept for at least five years and accessible only to authorised personnel and regulatory authorities.

5. Examples of Ongoing Monitoring in Practice

5.1. Scenario 1: Unusual Transaction Pattern

- **Detection:** The automated monitoring system detects large deposits followed by immediate withdrawals, which is inconsistent with the customer's usual activity.
- **Investigation:** The compliance team reviews the transactions and contacts the customer for an explanation. The customer provides documentation showing the transactions are related to a legitimate business deal.
- **Outcome:** After verifying the information, the transactions are deemed legitimate, but the customer's account is flagged for ongoing enhanced monitoring to detect any further unusual activity.

5.2. Scenario 2: High-Risk Customer Review

- **Detection:** A politically exposed person (PEP) conducts a large international transfer to a high-risk jurisdiction.
- **Investigation:** The compliance team initiates an enhanced due diligence process, including verifying the source of funds and the purpose of the transfer. Additional documentation is requested from the customer.

- **Outcome:** The transfer is approved after thorough verification, but the customer's account is subject to increased scrutiny, with all future transactions being reviewed by senior management.

5.3. Scenario 3: Periodic Information Update

- **Trigger:** A customer's periodic review is due. The compliance team requests updated identification documents and proof of address.
- **Review:** The customer's information is updated in the system, and their recent transactions are reviewed to ensure consistency with their profile.
- **Outcome:** The customer's profile is updated, and no suspicious activity is detected. The account continues to be monitored as per standard procedures.

6. Benefits of Ongoing Monitoring

- **Early Detection:** Enables early detection of suspicious activities, allowing Vortex FX to take prompt action to mitigate risks.
- **Regulatory Compliance:** Ensures compliance with AML regulations and reporting requirements, reducing the risk of regulatory penalties.
- **Customer Protection:** Protects customers from fraudulent activities by detecting and preventing unauthorised transactions.
- **Operational Integrity:** Maintains the integrity and reputation of Vortex FX by proactively managing and mitigating risks associated with financial crimes.

By implementing a robust ongoing monitoring process, Vortex FX ensures that customer activities are continuously scrutinised and potential risks are identified and addressed promptly. This approach not only enhances compliance with AML regulations but also strengthens the overall security and integrity of Vortex FX's financial services.

6. Reporting Suspicious Activity

Reporting suspicious activity is a critical element of Vortex FX's Anti-Money Laundering (AML) policy. This process ensures that any transactions or behaviours indicative of money laundering, terrorist financing, or other illicit activities are promptly identified, documented, and reported to the appropriate authorities. By doing so, Vortex FX helps combat financial crime and complies with regulatory requirements.

1. Key Components of Reporting Suspicious Activity

Detection of Suspicious Activity

- **Automated Monitoring Systems:** Vortex FX uses sophisticated automated systems to monitor transactions in real time. These systems are designed to detect patterns and

anomalies that may indicate suspicious activity.

- **Manual Review:** The compliance team conducts manual reviews in addition to automated systems to identify unusual or suspicious transactions that may not be flagged by automated systems.

1. **Transaction Red Flags:** Large, frequent, or unusual transactions that deviate from the customer's typical behaviour, transactions involving high-risk jurisdictions, and complex or structured transactions designed to evade reporting thresholds.

2. **Customer Behaviour Red Flags:** Reluctance to provide information, inconsistent or conflicting information, sudden changes in account activity, and use of multiple accounts or third parties to conduct transactions.

3. **Internal Reporting Process**
    - **Immediate Action:** When suspicious activity is detected, it is immediately reported to the designated AML compliance officer.
    - **Documentation:** Detailed records of the suspicious activity, including the nature of the transaction, the parties involved, and any supporting documentation, are compiled.
    - **Initial Assessment:** The compliance officer conducts an initial assessment to determine whether the activity warrants further investigation or immediate reporting to authorities.

4. **Investigation and Escalation**
    - **Enhanced Due Diligence:** Further investigation is conducted to gather additional information and verify the legitimacy of the suspicious activity. This may involve contacting the customer for an explanation and requesting additional documentation.
    - **Senior Management Review:** High-risk or complex cases are escalated to senior management for review and decision-making.
    - **Legal Consultation:** If necessary, legal counsel is consulted to ensure that the investigation and reporting comply with all applicable laws and regulations.

5. **Filing a Suspicious Activity Report (SAR)**
    - **SAR Preparation:** If the investigation confirms that the activity is suspicious and cannot be adequately explained, a Suspicious Activity Report (SAR) is prepared. The SAR includes detailed information about the activity, the parties involved, and the reasons for suspicion.
    - **Timely Filing:** The SAR is filed with the relevant financial regulatory authorities within the required timeframe, typically within 30 days of detecting the suspicious activity.

- **Confidentiality:** The process of filing a SAR is kept confidential, and the customer is not informed about the filing to avoid tipping off potential criminals.

6. **Follow-Up and Monitoring**
    - **Ongoing Monitoring:** Accounts associated with filed SARs are subject to increased scrutiny and ongoing monitoring to detect any further suspicious activity.
    - **Periodic Reviews:** The compliance team conducts periodic reviews of accounts and transactions to ensure that any additional suspicious activities are promptly identified and reported.
7. **Record Keeping**
    - **Documentation:** All records related to suspicious activity detection, investigation, and reporting are maintained for a minimum of five years. This includes copies of filed SARs and any supporting documentation.
    - **Audit Trail:** A comprehensive audit trail is maintained to document the steps taken during the investigation and reporting process.

2. Examples of Reporting Suspicious Activity

2.1. Scenario 1: Unusual Deposit and Withdrawal Pattern

- **Detection:** A customer deposits a large sum of money and immediately requests a wire transfer to an offshore account. This pattern deviates from their usual activity.
- **Investigation:** The compliance officer reviews the transaction, contacts the customer for an explanation, and requests additional documentation.
- **SAR Filing:** The customer's explanation is unsatisfactory, and the source of funds cannot be verified. A SAR is filed with the financial regulatory authorities, and the account is subject to increased monitoring.

2.2. Scenario 2: High-Risk Jurisdiction Transfer

- **Detection:** An existing customer initiates a large transfer to a high-risk jurisdiction known for weak AML controls.
- **Investigation:** Enhanced due diligence is conducted, including verifying the source of funds and the purpose of the transfer. The customer's background is also reviewed.
- **SAR Filing:** The investigation raises further concerns, and the transfer cannot be justified. A SAR is filed, and the customer's future transactions are closely monitored.

2.3. Scenario 3: Politically Exposed Person (PEP) Activity

- **Detection:** A Politically Exposed Person (PEP) makes several high-value deposits from unknown sources.
- **Investigation:** The compliance team conducts a thorough review, including checking international watchlists and verifying the source of funds.
- **SAR Filing:** The funds' origins remain unclear, and the transactions appear suspicious. A SAR is filed, and the customer is informed that their account will be under strict scrutiny.

Reporting Suspicious Activity

- **Compliance:** Ensures that Vortex FX complies with AML regulations and avoids regulatory penalties.
- **Risk Mitigation:** Helps mitigate the risk of being used as a conduit for money laundering and terrorist financing.
- **Reputation Protection:** Protects the reputation of Vortex FX by demonstrating a commitment to preventing financial crime.
- **Contribution to Global Efforts:** Contributes to global efforts to combat money laundering, terrorist financing, and other financial crimes by providing valuable information to authorities.

7. Training and Awareness

Training and awareness are critical components of Vortex FX's Anti-Money Laundering (AML) policy. Effective training ensures that employees at all levels understand their roles and responsibilities in preventing money laundering and terrorist financing. A well-informed workforce is essential for identifying and reporting suspicious activities, complying with regulatory requirements, and maintaining the integrity of Vortex FX's financial services.

1. Key Components of the Training and Awareness Program

1. **Training Programs:**
   - **Mandatory Training:** All employees, including new hires, must complete mandatory AML training as part of their onboarding process and at regular intervals thereafter.
   - **Role-Specific Training:** Customised training programs are developed based on the specific roles and responsibilities of employees. For example, front-line staff, compliance officers, and senior management receive training tailored to their functions and risk exposure.
2. **Training Content**

- **AML Regulations:** Training covers the latest AML laws and regulations applicable to Vortex FX, including international standards set by bodies such as the Financial Action Task Force (FATF).
- **Company Policies and Procedures:** Employees are trained on Vortex FX's internal AML policies, procedures, and controls, including customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring.
- **Red Flags and Indicators:** Training includes identifying red flags and indicators of suspicious activity, such as unusual transaction patterns, high-risk jurisdictions, and behaviours indicative of money laundering.
- **Reporting Procedures:** Employees learn the proper procedures for reporting suspicious activities, including how to complete and submit Suspicious Activity Reports (SARs) and the importance of maintaining confidentiality.
- **Case Studies and Scenarios:** Real-life case studies and hypothetical scenarios are used to illustrate common money laundering techniques and how to effectively respond to suspicious activities.

3. **Delivery Methods**
   - **E-Learning:** Online training modules allow employees to complete training at their own pace. These modules include interactive elements, quizzes, and assessments to reinforce learning.
   - **In-Person Training:** Workshops and seminars are conducted to provide hands-on training and facilitate discussions on AML topics. In-person sessions allow for immediate feedback and clarification of complex concepts.
   - **Webinars and Videos:** Webinars and instructional videos are used to deliver training to employees across different locations, ensuring consistent messaging and accessibility.
4. **Frequency of Training**
   - **Initial Training:** New employees complete their initial AML training within the first month of employment.
   - **Ongoing Training:** Refresher training is conducted annually to ensure employees remain up-to-date with the latest AML developments and company policies.
   - **Ad-Hoc Training:** Additional training sessions are scheduled as needed in response to changes in regulations, emerging risks, or identified weaknesses in AML controls.
5. **Assessment and Certification**
   - **Knowledge Assessments:** Employees are required to complete assessments at the end of each training module to evaluate their understanding of the material. Passing these assessments is mandatory for certification.

- **Certification:** Employees receive certification upon successful completion of their AML training. This certification is documented and tracked to ensure compliance with regulatory requirements.
- **Performance Reviews:** AML knowledge and compliance are incorporated into employee performance reviews, reinforcing the importance of AML responsibilities.

6. **Raising Awareness**
    - **Regular Updates:** Employees receive regular updates on AML issues, including changes in regulations, emerging threats, and best practices. These updates are disseminated through newsletters, emails, and the company intranet.
    - **Internal Communications:** Ongoing communications from senior management emphasise the importance of AML compliance and the Company's commitment to preventing financial crime.
    - **Awareness Campaigns:** Periodic awareness campaigns, such as AML awareness weeks or themed events, are organised to keep AML issues top of mind and encourage a culture of compliance.
7. **Monitoring and Evaluation**
    - **Training Effectiveness:** The effectiveness of the training program is regularly evaluated through feedback surveys, assessment results, and monitoring of compliance activities.
    - **Continuous Improvement:** Based on evaluation results, the training program is continuously updated and improved to address any gaps or areas for enhancement.
    - **Regulatory Compliance:** The training program is reviewed to ensure it meets all regulatory requirements and aligns with industry best practices.

2. Examples of Training and Awareness in Practice

2.1. Scenario 1: Front-Line Staff Training

- **Training Content:** Front-line staff, such as customer service representatives, receive training on identifying red flags during customer interactions, verifying customer identities, and reporting suspicious activities.
- **Delivery Method:** An e-learning module followed by an in-person workshop allows staff to practice identifying and responding to suspicious behaviours through role-playing exercises.

2.2. Scenario 2: Compliance Officer Training

- **Training Content:** Compliance officers receive advanced training on conducting enhanced due diligence, analysing complex transaction patterns, and filing SARs.

- **Delivery Method:** Webinars featuring industry experts and case studies provide in-depth knowledge and practical insights into handling high-risk scenarios.

2.3. Scenario 3: Senior Management Training

- **Training Content:** Senior management is trained on their oversight responsibilities, the importance of fostering a culture of compliance, and the strategic implications of AML policies.
- **Delivery Method:** A combination of executive briefings and interactive workshops ensures senior leaders are equipped to support and enforce AML initiatives.

Benefits of a Robust Training and Awareness Program

- **Enhanced Detection and Reporting:** Well-trained employees are better equipped to detect and report suspicious activities, reducing the risk of money laundering and terrorist financing.
- **Regulatory Compliance:** Comprehensive training ensures that Vortex FX complies with AML regulations and avoids potential fines and penalties.
- **Reputation Protection:** A strong commitment to AML training and awareness helps protect Vortex FX's reputation and build trust with customers, regulators, and stakeholders.
- **Employee Engagement:** Ongoing training and awareness initiatives foster a culture of compliance and accountability, empowering employees to take an active role in preventing financial crime.

8. Data Integrity Measures

We employ a comprehensive approach encompassing advanced technology, rigorous policies, and robust procedures to safeguard these records. Below is an overview of our data integrity measures and encryption practices:

1. Data Encryption

- **In-Transit Encryption:** All data transmitted over networks is encrypted using industry-standard protocols such as Transport Layer Security (TLS). This encryption prevents unauthorised interception and ensures that data remains confidential during transmission.
- **At-Rest Encryption:** Sensitive data stored in our databases is protected using strong encryption algorithms, specifically AES-256 (Advanced Encryption Standard with 256-bit keys). This high-level encryption safeguards data against unauthorised access and potential breaches.

2. Access Controls

- **Role-Based Access Control (RBAC):** Access to sensitive data is restricted based on job roles and responsibilities. This ensures that only authorised personnel have access to data necessary for their roles, minimising the risk of data exposure.

- **Multi-Factor Authentication (MFA):** MFA is mandatory for accessing systems that handle sensitive information, adding an extra layer of security by requiring multiple forms of verification.
- **Audit Trails:** Comprehensive audit logs are maintained to record access and actions performed on sensitive data. These logs ensure accountability and traceability, helping to detect and respond to unauthorised access.

3. Data Integrity Measures

- **Hashing:** Critical data elements are hashed to detect any unauthorised changes or tampering. Regular comparison of hash values ensures that data remains unaltered and intact.
- **Checksum Verification:** Files and data transmissions include checksums that are verified upon receipt. This process ensures that the data has not been corrupted or altered during transmission.

4. Regular Security Audits and Assessments

- **Internal Audits:** Regular internal audits are conducted to review data security practices, access controls, and compliance with internal policies. These audits help identify potential vulnerabilities and areas for improvement.
- **External Audits:** Periodic external audits by independent security firms verify the effectiveness of our security measures and ensure compliance with industry standards.
- **Vulnerability Assessments:** Routine vulnerability assessments and penetration testing are conducted to identify and mitigate potential security weaknesses.

5. Data Backup and Recovery

- **Regular Backups:** Critical data is backed up regularly using secure methods to ensure that it can be restored in the event of data loss or corruption.
- **Disaster Recovery Plan:** A comprehensive disaster recovery plan is in place to ensure business continuity and data integrity in case of system failure or security incidents.
- **Redundancy:** Data is stored in redundant locations to protect against data loss from physical damage or system failures.

6. Compliance with Data Protection Regulations

- **GDPR Compliance:** Vortex FX adheres to the General Data Protection Regulation (GDPR) for handling personal data, ensuring that data protection principles are followed meticulously.
- **Data Protection Officer (DPO):** Our DPO oversees compliance with data protection regulations and advises on best practices for data security and privacy.

7. Employee Training and Awareness

- **Security Training:** Employees receive regular training on data security practices, including recognising phishing attempts, handling sensitive information, and reporting security incidents.
- **Confidentiality Agreements:** All employees and contractors sign confidentiality agreements as part of their employment contracts, legally binding them to protect sensitive information.

8. Secure System Design

- **Secure Development Practices:** Our software development follows secure coding practices, including regular code reviews and security testing, to ensure the robustness of our systems.
- **Security by Design:** Systems and processes are designed with security in mind from the outset, integrating robust protection measures to safeguard data.

9. Incident Response Plan

- **Incident Handling:** A formal incident response plan is in place to manage and mitigate the impact of data breaches or security incidents promptly.
- **Reporting and Remediation:** Incidents are promptly reported, investigated, and remediated. Lessons learned from incidents are used to improve security measures continuously.

10. Third-Party Risk Management

- **Vendor Assessments:** Thorough assessments of third-party vendors are conducted to ensure they meet Vortex FX's stringent security and confidentiality standards.
- **Contracts and SLAs:** Contracts with third parties include specific data protection and security requirements. Service Level Agreements (SLAs) are monitored for compliance to ensure ongoing adherence to these standards.

9. Record Keeping

Effective record-keeping is a cornerstone of Vortex FX's Anti-Money Laundering (AML) policy. Maintaining comprehensive and accurate records ensures compliance with regulatory requirements, supports the monitoring and investigation of suspicious activities, and preserves the integrity of Vortex FX's financial operations.

Proper record-keeping facilitates transparency, accountability, and the ability to provide necessary information to regulatory authorities upon request.

1. Key Components of Record-Keeping

1. **Types of Records Maintained**
    - **Customer Identification Records:** Documentation and information collected during the customer due diligence (CDD) and enhanced due diligence (EDD) processes, including identification documents, proof of address, and beneficial ownership details.
    - **Transaction Records:** Detailed records of all customer transactions, including deposits, withdrawals, transfers, and other financial activities. This includes the date, amount, currency, and purpose of each transaction, as well as the parties involved.
    - **Monitoring and Reporting Records:** Records related to the monitoring of customer activities and transactions, including alerts generated by automated systems, investigations conducted, and Suspicious Activity Reports (SARs) filed.
    - **Training Records:** Documentation of AML training provided to employees, including attendance records, training materials, and assessments completed.
    - **Compliance Reviews and Audits:** Records of internal and external audits, compliance reviews, and any actions taken to address identified issues or weaknesses.
2. **Retention Periods**
    - **Minimum Retention Period:** All AML-related records must be retained for a minimum of five years from the date of the transaction or the end of the business relationship, whichever is later.
    - **Extended Retention:** In cases where an investigation is ongoing, records must be retained until the investigation is concluded and any regulatory requirements are fully satisfied.
3. **Accessibility and Retrieval**
    - **Secure Storage:** Records are stored securely to prevent unauthorised access, alteration, or destruction. Both physical and electronic records are protected using appropriate security measures.

- **Ease of Retrieval:** Records are organised and indexed to ensure they can be easily retrieved when needed, whether for internal review, regulatory examination, or legal proceedings.

4. **Accuracy and Completeness**
   - **Data Quality Controls:** Procedures are in place to ensure the accuracy, completeness, and reliability of records. This includes regular reviews and updates of customer information and transaction details.
   - **Error Correction:** Any identified errors or discrepancies in records are promptly corrected, and measures are taken to prevent recurrence.
5. **Confidentiality and Data Protection**
   - **Confidentiality:** All AML-related records are treated as confidential and are accessible only to authorised personnel. Employees are trained on the importance of maintaining confidentiality and the potential consequences of breaches.
   - **Data Protection:** Compliance with data protection regulations, such as the General Data Protection Regulation (GDPR), ensures that customer information is handled responsibly and privacy rights are respected.
6. **Audit and Review**
   - **Internal Audits:** Regular internal audits are conducted to assess the effectiveness of the record-keeping processes and identify any areas for improvement. All audit logs are retained.
   - **External Audits:** Periodic external audits by independent auditors provide an additional layer of assurance regarding the adequacy and compliance of the record-keeping system.
7. **Regulatory Compliance**
   - **Regulatory Requests:** Vortex FX is prepared to promptly respond to requests for information from regulatory authorities. This includes providing access to records related to specific customers, transactions, or investigations.
   - **Compliance Documentation:** Detailed documentation of compliance activities, including policies, procedures, and records of regulatory interactions, is maintained to demonstrate adherence to AML regulations.

2. Examples of Record Keeping in Practice

2.1. Scenario 1: Customer Identification Records

- **Record Keeping:** During the account opening process, a customer provides their passport, proof of address, and information on beneficial ownership. These documents are scanned and securely stored in the electronic customer file.

- **Retention:** The records are retained for at least five years after the business relationship ends, ensuring they are available for any future regulatory inquiries.

2.2. Scenario 2: Transaction Records

- **Record Keeping:** A customer makes several large deposits and international transfers. Each transaction is recorded in detail, including the date, amount, currency, destination, and purpose of the transfer.
- **Monitoring:** The transactions are flagged for review due to their size and frequency, and the compliance team conducts an investigation. All findings and actions taken are documented and stored.

2.3. Scenario 3: Suspicious Activity Reporting

- **Record Keeping:** A suspicious transaction is detected, and a SAR is filed with the relevant authorities. The SAR and all related documentation, including the initial alert and investigation notes, are securely stored.
- **Confidentiality:** The SAR is kept confidential, with access restricted to authorised personnel only.

2.4. Benefits of Effective Record Keeping

- **Regulatory Compliance:** Ensures compliance with AML regulations and avoids potential fines or penalties for record-keeping deficiencies.
- **Enhanced Monitoring:** Supports ongoing monitoring efforts by providing a comprehensive record of customer activities and transactions.
- **Facilitated Investigations:** Enables efficient and thorough investigations of suspicious activities, ensuring that necessary information is readily available.
- **Transparency and Accountability:** Promotes transparency and accountability within Vortex FX, demonstrating a commitment to preventing financial crime.
- **Operational Integrity:** Protects the integrity of Vortex FX's financial operations by maintaining accurate and reliable records.

10.Non-Compliance

Employees are expected to adhere to the policies and procedures outlined in this document and those referenced within it.

Should an employee be found in breach of these policies, they may face disciplinary measures, which could include termination of employment.

Monitoring and Reviewing

Vortex FX is committed to ensuring our policies are effective and up-to-date. To do this, we have a process for regularly monitoring and reviewing them.

Our Senior Managers and Directors are responsible for this process and will review the policies at least once a year or more frequently if needed due to changes in laws or our practices.

11.Monitoring and Reviewing

Vortex FX is committed to ensuring our policies are effective and up-to-date. To do this, we have a process for regularly monitoring and reviewing them.

Our Directors are responsible for this process and will review the policies at least once a year or more frequently if needed due to changes in laws or our practices.