AML Policy (Anti-Money Laundering)

1. The Anti-Money Laundering (AML) and Counter-Terrorism Funding Policy of **Xellion Ltd** (collectively referred to herein as “the company”, “our”, “us”, “we” or “Xellion”) is designed to comply with internationally recognized standards, including the **EU Anti-Money Laundering Directives (AMLD)**, the **Financial Action Task Force (FATF) Recommendations**, and the **Saint Lucia Anti-Money Laundering (AMLCFT) Act**. Our objective is to ensure that our platform is not used to facilitate any form of money laundering or terrorist financing. The Company enforces a strict **zero-tolerance policy** for such activities.

2. The Company takes AML seriously, and any violation of our policies will result in immediate action. The Company reserves the right to refund, deny, or withhold any deposit that is in breach of this policy or reasonably suspected—based on applicable law or internal procedures—to be associated with illegal activity (e.g., transfers from high-risk jurisdictions, structuring, etc.).

KYC Policies (Know Your Client)

KYC – Identification and Verification of New Customers, Deposits, Transfers, and Withdrawals

1. In order to open an account with the Company, the client must submit:
    - Surname
    - First Name
    - National ID or Passport Number
    - Address
    - Email
    - Telephone
2. The client must also submit a valid identification document. Depending on internal risk-based assessment, this document may be required to include:
    - Photo of the holder
    - ID number

- Full name
- Parent names
- Date and place of birth
- Gender
- Residential address
- Marital status
- Spouse details (where applicable)

3. Further verification steps are triggered upon initial deposit. All accounts must be in the **same name** as the person funding the account. **Third-party payments are strictly prohibited.**

4. The Company conducts **manual verification** of all documents submitted by clients or, where applicable, utilizes an **automated KYC platform** operated by a third-party provider specialized in identity verification, document validation, and fraud detection.

5. Verification includes matching credit card or bank transfer data with submitted identity documentation. Accounts are activated only after successful verification. Any inconsistency will result in a rejection and refund to the original payment source.

6. All credit card deposits are subject to the fraud and AML checks of our licensed credit card processing partner.

7. Withdrawals are only allowed to **the exact same source and name** used for the original deposit. **No third-party withdrawals** are permitted.

8. The withdrawal method must also **match the original deposit method**. For example, deposits via credit card will be refunded back to that same card, up to the original amount.

9. Repeat credit card users or clients depositing more than **$5,000** in total will be subject to enhanced due diligence procedures.

10. Withdrawals are processed only upon receipt of a signed written request and verified proof that the beneficiary account belongs to the client.

11. The Company reserves the right to request further identification if a red flag is triggered during onboarding, activity monitoring, or transaction reviews.

12. Suspicious behavior—such as unusual transfer patterns or frequent small deposits—will be monitored continuously.

13. KYC verification is completed **at or shortly after account creation** using document-based and non-document-based methods (e.g., liveness check, database cross-reference).

14. If the Company is **unable to establish a reasonable belief** of a client's identity, the account will not be opened. Our systems do not allow the creation of accounts without successful identity verification.

15. All identification records will be **retained for a minimum of five (5) years**, including digital copies or structured records of submitted documents and any information used to resolve discrepancies.

16. **Xellion Ltd** reserves the right to **verify documents within 2 business days** and may request additional supporting documentation when initial data is insufficient.

17. The Company may also request, at its discretion, further documentation at any stage to validate actions related to deposits, withdrawals, or refunds.

Detecting and Reporting Suspicious Activity

18. For **high-risk clients or transactions**, additional enhanced due diligence (EDD) will be applied. This may include requests for bank references, certified documents, direct client interviews, or video calls.

19. Additional monitoring of account activity will be performed when deemed necessary based on client profile, geography, or transaction history.

20. Internal systems are maintained to **detect, flag, and escalate suspicious activity** in compliance with applicable regulatory requirements and international AML standards.