

Know Your Customer (KYC) Policy

1. Introduction.

Know Your Customer (KYC) Policy is to prevent and mitigate the risks of money laundering, terrorist financing, and other financial crimes. Top Magic Limited (the “**Company**”) is committed to ensuring compliance with all relevant UK regulations and international standards.

KYC concerns all employees, contractors, consultants, temporary and agency staff, and any other individuals working for or on behalf of Top Magic Limited and it covers all customer interactions, including account opening, ongoing monitoring, and transaction processing.

2. Regulatory Framework.

This Policy is based on the following UK and international regulations and standards, as amended and in force:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
- The Proceeds of Crime Act 2002 (POCA).
- The Terrorism Act 2000.
- The Financial Conduct Authority (FCA) guidelines.
- The Joint Money Laundering Steering Group (JMLSG) guidance.
- Relevant EU directives and international standards (e.g., FATF recommendations).

3. Policy Statement.

The Company is committed to:

- Identifying and verifying the identity of customers and beneficial owners.
- Understanding the nature and purpose of customer relationships.
- Conducting ongoing monitoring of customer transactions and activities.
- Reporting suspicious activities to the appropriate authorities.

4. Customer Identification & Verification.

4.1 Customer Due Diligence (CDD):

A. Obtain and verify the following information for individual customers:

- Full name
- Date of birth
- Residential address
- Nationality
- Identification documents (e.g., passport, driving licence)

B. Obtain and verify the following information for corporate customers:

- Company name
- Registered office address
- Business address (if different)
- Nature of business
- Names of directors and beneficial owners
- Identification documents for directors and beneficial owners

4.2 Enhanced Due Diligence (EDD):

A. Apply enhanced measures for high-risk customers, including:

- Politically Exposed Persons (PEPs)
- Customers from high-risk jurisdictions
- Complex ownership structures
- Unusual or large transactions

B. Additional measures may include:

- Obtaining additional identification documents
- Conducting enhanced background checks
- Monitoring transactions more closely

5. Risk Assessment.

5.1 Conduct a risk assessment of each customer based on factors such as:

- Customer type (individual, corporate, PEP)
- Geographical location
- Nature and purpose of the business relationship
- Transaction patterns and volumes

5.2 Assign a risk rating (low, medium, high) and apply appropriate due diligence measures.

6. Ongoing Monitoring.

- Monitor customer transactions and activities on an ongoing basis to detect unusual or suspicious patterns.
- Update customer information and risk assessments regularly.
- Review and analyse transactions against known patterns of money laundering and terrorist financing.

7. Record Keeping.

- Maintain records of all customer identification and verification documents for at least five (5) years after the end of the business relationship.
- Keep records of all transactions and customer interactions for at least five (5) years.
- Ensure records are accessible, secure, and retrievable.

8. Reporting Suspicious Activities.

- Identify and report suspicious activities to the Line Manager.
- The Line Manager will review and, if necessary, file a Suspicious Activity Report (SAR) with the National Crime Agency (NCA).
- Maintain confidentiality and do not disclose the existence of a SAR to the customer.

9. Training & Awareness.

- Provide regular training to employees on KYC procedures, money laundering risks, and reporting obligations.
- Ensure employees are aware of the importance of KYC compliance and the consequences of non-compliance.

10. Policy Review.

- Review this Policy annually and update it as necessary to ensure compliance with changing regulations and standards.
- Incorporate feedback from employees, customers and regulatory authorities in Policy updates.

Last Updated: 05 February 2026