KYC/AML POLICY

Updated: March 6, 2026

Pursuant to a software license agreement, TASKITT LTD operates URL: www.sweepstakesonline.com(hereinafter “Service Provider”) Know Your Customer (“KYC”) and Anti-Money Laundering (AML) Policy.

General Provisions

1.1. This Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) Policy, along with the adherence to international sanctions (hereinafter, the Policy), establishes the requirements for Users and Transaction verification to prevent transactions related to suspected money laundering and terrorist financing, as well as to ensure the identification and reporting of such cases.

1.2. The purpose of this KYC policy is to establish a framework for verifying the identity of customers who use Service Provider’s URL: www.sweepstakesonline.com. This policy ensures compliance with relevant legal and regulatory requirements, helps prevent fraudulent activities, and promotes a secure and trustworthy gaming environment.

1.3. Compliance with the Policy is the responsibility of the Chief Executive Officer (CEO) and the Service Provider's employees, including temporary personnel and agents, who initiate or establish Business Relationships (as defined in Section 5), collectively referred to as Representatives. Each Representative is required to confirm familiarity with the Policy by signature.

1.4. The Policy sets forth standards defined in accordance with the principles contained in the Law of United States of America on the Facilitation of the Prevention of Illicit Income Legalization, and international best practices to prevent the misuse of the financial system for money laundering and terrorist financing.

Objectives

- Verify the identity of customers (KYC)
- Monitor and report suspicious activities.
- Ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.
- Protect the website from fraudulent activities.
- Safeguard customer data in accordance with privacy laws.

Scope

This KYC and AML policy applies to all customers who register, participate, and conduct transactions on www.sweepstakesonline.com. It includes the processes for customer identification, verification, and ongoing monitoring.

Definitions

2.1. Money Laundering – a set of actions involving property obtained from criminal activity or property acquired in exchange for such property, intended to:

i. Conceal or disguise the true nature, source, location, disposition, movement, ownership, or rights associated with such property;
ii. Convert, transfer, acquire, possess, or use such property to conceal or disguise its illegal origin or to help a person involved in criminal activity avoid the legal consequences of their actions;
iii. Participate in, facilitate, attempt, assist, instigate, aid, or advise in the performance of any acts listed in subsections 2.1.i and 2.1.ii.

2.2. Terrorist Financing – the provision or collection of funds for a terrorist or terrorist organization with the intention of using them or knowingly and voluntarily knowing that they will be used, even without connection to a specific act, in whole or in part, to commit acts classified as crimes under the law.

2.3. International Sanctions – a set of non-military measures imposed by the European Union, United Nations, Office of Foreign Assets Control (OFAC), or other international organizations or the government of the United States aimed at maintaining or restoring peace, preventing conflicts, and restoring international security, supporting and strengthening democracy, upholding the rule of law, human rights, and international law.

2.4. Compliance Officer – a representative appointed by the CEO responsible for the effective implementation of the Policy.

2.5. Business Relationship – a relationship established by the Service Provider in its economic and professional activities with a Customer.

2.6. Transaction – a monetary flow or payment order, bank transfer, credit/debit card payment, or cryptocurrency transfer from the Customer to the Service Provider.

2.7. Representative— Director, Managers, and Employees.

2.8. Customer – an individual or legal entity utilizing the Service Provider's product.

2.9. Beneficial Owner – an individual who:

i. Exercises control over a transaction, operation, or another person for whose benefit, on whose behalf, or in whose account the transaction or operation is conducted;

ii. Ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of shares or votes, including bearer shares, or by exercising control by other means. Direct ownership is a form of control where an individual owns 25 percent plus one share or more than 25 percent of a company's stake. Indirect ownership is a form of control where a company controlled by an individual or multiple companies controlled by the same individual owns a 25 percent plus one share or more than a 25 percent stake in a company.

iii. Holds a senior management position if, after exhausting all possible identification means, the person specified in subsection ii cannot be identified and there is no doubt about their existence, or if doubts arise about the identified person as the Beneficial Owner.

iv. In the case of a trust, civil partnership, association, or legal agreement, the Beneficial Owner is he individual who ultimately controls the association through direct or indirect ownership or otherwise, and is: the founder or person who transferred the property to the property pool, manager or property holder, person providing and controlling property security, if designated, or the beneficiary, or if the beneficiary or beneficiaries are not yet determined, the class of persons for whose benefit the association is established or operates.

2.9. Politically Exposed Person (PEP) – an individual entrusted with or previously entrusted with prominent public functions, including the head of state, head of government, minister, or deputy or assistant minister; a member of parliament or similar legislative body, member of the governing body of a political party, member of the supreme court, member of the court of auditors or board of a central bank; ambassador, senior military officer; member of an administrative, managerial, or supervisory body of a state-owned enterprise; director, deputy director, and member of the board or
equivalent position in an international organization, excluding middle and lower levels.

2.9.1. Family member of a PEP – a spouse or equivalent partner, children and their spouse or equivalent partner, and parent of a PEP.

2.9.2. Close associate of a PEP – an individual known as a beneficial owner or holding joint beneficial ownership with a PEP in a legal entity or legal arrangement, or having other close business relations with a PEP; also, an individual holding sole beneficial ownership of a legal entity or arrangement known to be established for the benefit of a PEP.

2.10. Service Provider: www.sweepstakesonline.com, providing services for online sweepstakes gaming.

Compliance Officer

3.1. The CEO appoints the Compliance Officer (CO), whose primary responsibilities include:

3.1.1. Monitoring adherence to the Policy with current legislation and compliance by Representatives with the procedures established in the Policy;

3.1.2. Collecting and updating information on countries with low tax risk, high and low risks of money laundering and terrorist financing, and economic activities with high money laundering and terrorist financing risks;

3.1.3. Conducting training, briefings, and updating Representatives on KYC/AML/CFT procedures;

3.1.4. Reporting to the CEO annually (or more frequently if necessary) on Policy compliance and Transactions with suspected money laundering or terrorist financing;

3.1.5. Collecting, processing, and analyzing data received from Representatives or Customers regarding suspicious and unusual activities;

3.1.6. Reporting cases of suspected money laundering or terrorist financing and responding to inquiries from relevant federal and state authorities;

3.1.7. Proposing solutions to eliminate identified deficiencies during audits.

Customer Due Diligence (CDD)

4.1. The Service Provider defines and applies CDD measures based on the results of a risk assessment conducted.

4.2. Representatives should pay special attention to Customer actions involved in Transactions and circumstances indicating money laundering or terrorist financing, including complex, large, or unusual Transactions with no reasonable economic purpose.

4.3. Depending on the risk level of the Customer and/or Transaction, and whether the Business Relationship is existing or new, the Service Provider applies standard CDD measures (see Section 5), simplified CDD measures (see Section 8), or enhanced CDD measures (see Section 9). The Service Provider also applies ongoing CDD measures to ensure continuous monitoring of Business Relationships.

4.4. CDD measures include the following procedures:

i. Identification of the Customer and verification of their identity using reliable, independent sources, documents, or data, including electronic identification;

ii. Identification and verification of the Customer’s representative and their authority to represent the Customer;

iii. Identification of the Beneficial Owner of the Customer;

iv. Assessment and, if necessary, collection of information on the purpose of the Business Relationship and Transaction;

v. Ongoing monitoring of the Customer’s business to ensure the Transactions conducted are consistent with the Service Provider's knowledge of the Customer and their source of funds;

vi. Obtaining information on whether the Customer is a PEP, a family member of a PEP, or a close associate of a PEP.

4.5. The Service Provider establishes the source of the Customer’s wealth if appropriate.

4.6. To fulfill the CDD obligation, Representatives have the right and are obliged to:

i. Request relevant documents to identify the Customer and their representatives;

ii. Request documents and information regarding the Customer’s activities and the legitimate origin of funds;

iii. Request information about the Beneficial Owners of a legal entity;

iv. Assess the risk profile of the Customer/Transaction, choose appropriate CDD measures, and evaluate whether the Customer or another party related to the Transaction may be involved in money laundering or terrorist financing;

v. Re-identify the Customer or their representative if doubts arise about the accuracy of the information obtained during initial identification;

vi. Refuse to engage in or complete a Transaction if there is suspicion that the Transaction is related to money laundering or terrorist financing or that the Customer or another party related to the Transaction is or may be involved in money laundering or terrorist financing.

4.7. The purpose of ongoing CDD is to ensure continuous monitoring of Customer and Transactions. Continuous monitoring of Business Relationships includes:

i. Reviewing Transactions to ensure they align with the Service Provider's knowledge of the Customer, the Customer's business, and risk profile;

ii. Obtaining information about the sources of funds for Transactions;

iii. Updating documents, data, or information obtained when applying CDD measures;

iv. Paying special attention to Transactions and Customer actions that could lead to criminal activity or money laundering or terrorist financing, and clarifying the nature, purpose, and background of such Transactions;

v. Paying special attention to Business Relationships or Transactions if the Customer or the Customer's legal entity is located in a third country included on the list of high-risk countries.

4.8. An annual review of the legal status of the Customer's legal entity is conducted regularly once a year. Updated data is recorded in the Service Provider's Customer database.

4.9. The Representative updates Customer data, whether for a legal entity or individual, i.e., takes appropriate CDD measures each time:

i. The Customer requests the Service Provider to change a long-term contract during its term;

ii. Identification and verification raise grounds for suspecting that previously collected documents or data are insufficient, outdated, or incorrect. In this case, the Representative may conduct a personal meeting with the Customer;

iii. The Customer's Transaction data shows significant changes in the Customer's business activity or volume, requiring a change in the Customer's risk profile;

iv. The Service Provider learns through third parties or media that the Customer's activity or information has significantly changed.

4.10. The Representative assesses the nature and purpose of the Customer's activity to establish possible connections of the relevant Transaction with money laundering or terrorist financing. The assessment should lead to an understanding of the Business Relationship's purpose for the Customer, the Customer's business nature, the Customer's risk levels, and, if necessary, the sources of funds associated with the Transactions.

Standard Due Diligence Measures

5.1. The Service Provider conducts standard CDD measures in the following cases:

i. When establishing new Business Relationships;

ii. If a single Transaction amount exceeds 2,000 USD;

iii. If previously collected documents or information are insufficient or suspected to be incorrect during the CDD process; and

iv. If there is a suspicion of money laundering or terrorist financing.

5.2. During standard CDD measures, the Representative applies the CDD procedures outlined in Section 4.4.

5.3. New Business Relationships cannot be established, and a Transaction cannot be completed if the Customer, despite an appropriate request, has not provided the documents and necessary information for CDD or if the documents presented by the Representative raise suspicions of money laundering or terrorist financing.

5.4. If an existing Customer, despite an appropriate request, has not provided the documents and necessary information for CDD during the contract term, this behavior is a material contract violation, which must be reported by the Representative, and in such cases, contracts with the Customer must be terminated, and Business Relationships discontinued as soon as possible.

5.5. The Service Provider does not enter into Business Relationships with anonymous Customers.

Customer Identification Program (CIP).

6.1 Information Collection

During registration, customers must provide the following information:
i. Full name and Date of birth;
ii. Residential address;
iii. Email address;
iv. Phone number
v. Current Government-issued photo ID (e.g., passport, driver's license)
vi. Biometric identification

6.2. Verification Process

6.3. Document Verification: Customers must upload a government-issued photo ID for verification. The document will be checked for authenticity and validity using third-party software and vendor to identity Customer.

6.4. Address Verification: Customers may be required to provide additional documents, such as utility bills or bank statements, to verify their residential address.

6.5. Electronic Verification: The provided information will be cross-checked against public and private databases to confirm identity and address.

6.6. The Service Provider will use a third-party software and vendor to identity Customer's geolocation.

7.0 Risk-Based Approach

The Service Provider has adopted a risk-based approach to combat money laundering and terrorist financing, in line with international requirements. By adopting a risk assessment-based approach, the Service Provider can ensure that measures to prevent or mitigate money laundering and terrorist financing are proportionate to the identified risks, allowing resources to be allocated most effectively. The guiding principle is that resources should be directed according to priorities, with the greatest attention given to the highest risks.

Customers will be categorized based on their risk profiles:

Low Risk: Customers with consistent behavior and low transaction volumes.
Medium Risk: Customers with irregular transactions or higher volumes.
High Risk: Customers from high-risk jurisdictions or with significant changes in behavior.

Suspicious Transaction Reporting

8.1. Notification of the Compliance Officer

8.1.1. If unusual or suspicious circumstances are identified in the Business Relationship, or there are characteristics indicating money laundering, terrorist financing, or an attempt of such actions, the CEO, Director, Managers, or Employees must promptly notify the Compliance Officer ("CO").

8.1.2. The CO must analyze and forward the relevant information to the CEO.

8.2. Notification of Official State Authorities

8.2.1. The CO is authorized to decide whether a transaction is suspicious and, accordingly, to report the information to the relevant official state or federal authorities, while the CEO decides whether to suspend the Transaction and/or terminate the Business Relationship.

8.2.2. The CO must retain all reports received from Representatives about suspicious and unusual Transactions in a reproducible written format, along with all information gathered for

analyzing such notifications, and other related documents and notifications, including the time of the notification and information about the Representatives who submitted it.

8.2.3. The Customer or individual involved in the Transaction (including their representative and other related individuals) reported as suspicious cannot be informed of this.

9.0. Ongoing Monitoring

9.1. Transaction Monitoring: All transactions will be monitored for unusual or suspicious activities. Transactions exceeding predefined thresholds will trigger further verification and investigation.

9.2. Periodic Review: Customer information will be periodically reviewed and updated to ensure accuracy. High-risk customers will undergo more frequent reviews.

9.3. Record Keeping

All customer identification and verification records will be securely stored for at least five years. Records of transactions and interactions with customers will also be maintained for the same period. Customer data will be handled in compliance with GDPR and other relevant privacy laws. Strong encryption and access controls will be implemented to protect customer information.

10.0 Compliance Officer

A dedicated Compliance Officer will oversee the implementation of the KYC and AML policy, handle regulatory reporting, and ensure ongoing compliance. The service provider has a law firm on monthly retainer to train, monitor, and enforce the KYC and AML policy. Should the law firm cease this role, the law firm will notify the merchant processor with 48 hours after to notice to the CEO.

11.0 Employee Training

Regular training sessions will be conducted for employees to ensure they understand KYC and AML requirements and can effectively implement the policy. Employees will be trained to identify and report suspicious activities.

12.0. Policy Review and Updates

The KYC and AML policy will be reviewed annually and updated as necessary to comply with new regulations and emerging best practices. Feedback from stakeholders, including customers and employees, will be incorporated into the policy review process.

13.0. Approval and Authority

The KYC and AML policy is approved by the CEO and is enforced across all levels of the organization. The Compliance Officer has the authority to make necessary decisions to ensure the policy's effective implementation.

[*nothing more follows]*

©TASKITT LTD, URL:www.sweepstakesonline.com

(2025). All Rights Reserved.