

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM POLICY

INTERSEAL B.V.

Registration number: 163945



Stanislav Andrieiev, the
MLRO & Compliance
Officer



**Jonathan Marshall Ruwel
Heymans** obo Kurason Trust
Curacao N.V., the Managing
Director

CONTENTS

1.	GENERAL PROVISIONS AND POLICY STATEMENT.....	4
2.	AUDIENCE	5
3.	DEFINITIONS AND ABBREVIATIONS.....	6
4.	BUSINESS RISK ASSESSMENT	7
5.	CUSTOMER RISK ASSESSMENT	9
6.	CUSTOMER ACCEPTANCE POLICY.....	10
7.	CUSTOMER DUE DILIGENCE	10
8.	COUNTER-PARTY DUE DILIGENCE	13
9.	ENHANCED MONITORING AND DUE DILIGENCE	15
10.	ONGOING DUE DILIGENCE (MONITORING).....	17
11.	RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE.....	19
12.	RISK PROFILES.....	19
14.	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE. TERMINATION OF BUSINESS RELATIONSHIP AND ASSETS FREEZE.....	20
15.	REPORTING OF SUSPICIONS	21
16.	RECORDING AND REPOTING	22
17.	COOPERATION WITH AUTHORITIES	24
18.	OTHER MESURES	24
19.	THE COMPLIANCE OFFICER (MONEY LAUNDERING REPORTING OFFICER (MLRO): APPOINTMENT AND RESPONSIBILITIES.	25
20.	TRAINING	27
21.	NOTIFICATIONS.....	28
22.	UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION	28
23.	CONTACT INFORMATION	29
24.	POLICY HISTORY.....	29

KEY INFORMATION

Approving Official(s):	Stanislav Andrieiev, the MLRO & Compliance Officer Jonathan Marshall Ruwel Heymans obo Kurason Trust Curacao N.V., the Managing Director
Responsible Office:	Stanislav Andrieiev, the MLRO & compliance officer
Effective Date:	19.05.2025
Next Review Date:	19.05.2026

1. GENERAL PROVISIONS AND POLICY STATEMENT

- 1.1. The company is ensuring that the business is conducted at a high ethical standard and that the laws and regulations pertaining to financial transactions are followed.
- 1.2. *Subject matter, including the scope and applicability.* Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable FATF, GCB regulations general AML rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.
- 1.3. *Purpose.* The purpose of this Policy is to make and enhance the legal framework and practices that our Company should implement to prevent, detect, and report money laundering activities. The primary goal is to prevent illicit funds from being processed through our casino financial systems. In addition, this Policy encompasses the regulations and policies designed to prevent our Company and casino from being used as a conduit for terrorism financing. The aim is to ensure that funds are not channeled to support terrorist activities.
- 1.4. The Company shall monitor this Policy with legal and regulatory requirements and conduct an annual independent AML/CFT compliance audit, the findings of which are to be considered and appropriate recommendations for action set out. The Company shall provide the necessary authority and resources for the ongoing implementation of a compliant AML regime.
- 1.5. The Company developing the training programs and provide training to all personnel who perform transactions as referred to in the NOIS and the NORUT. Training includes setting out rules of conduct governing employees' behavior and their ongoing education to create awareness of the Company's policy against money laundering and terrorist financing.
- 1.6. Preventing money laundering or terrorist financing (ML/TF) is more effective in protecting communities from harm than pursuing prosecution of the activity after it happens. We are required by law to implement anti-money laundering (AML) and counter-terrorism financing (CTM) measures. This compliance is mandated by national laws, such as the Bank Secrecy Act in the United States or the EU's Anti-Money Laundering Directives, as well as international frameworks set by entities like the Financial Action Task Force (FATF). Non-compliance can result in hefty fines, loss of licenses, and even criminal charges for the operators of the online casinos. These regulations exist to ensure that gambling operations are not used as vehicles for laundering illicit proceeds or financing terrorism.
- 1.7. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.
- 1.8. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used

by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

- 1.9. The FATF defines proliferation of weapons of mass destruction (WMD) as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. The issue of proliferation received international attention for several years. A number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials (such as the Nuclear Non-Proliferation Treaty). These treaties do not, however, consider the aspect of financing proliferation. The interconnection is based on the fact that proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied in order to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing. Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.
- 1.10. The Company is entitled to engage third parties to perform certain functions related to AML/CFT subject to confidentiality.
- 1.11. No member of staff shall at any time disclose a money laundering suspicion to the person suspected, whether or not a client, or to any outside party. If circumstances arise that may cause difficulties with client contact, the member of staff must seek and follow the instructions of the Responsible person.

2. AUDIENCE

- 2.1. This policy affects and regulates:
 - 2.1.1. Casino Management and Staff. Senior management and operations staff are directly involved in implementing and overseeing AML and CTM policies. This includes understanding the requirements, ensuring compliance, and creating a culture of vigilance and ethical conduct within the Company.
 - 2.1.2. Compliance Officers. Individuals responsible for developing, implementing, and monitoring our compliance program. They ensure that our Company adheres to relevant laws and regulations and often serve as the primary liaison between the casino and regulatory authorities.
 - 2.1.3. Technology and IT Teams. These teams implement and manage technology solutions that support transaction monitoring, customer due diligence, and reporting systems essential for AML and CTM compliance.
 - 2.1.4. Customers. Although not directly involved in policy creation, customers are a crucial audience as policies impact their interaction with the casino and our Company. These policies ensure customer transactions are safe and legitimate, thus building trust in the casino's operations and our Company.
 - 2.1.5. Investors and Stakeholders. Investors and our stakeholders have a vested interest in the compliance with AML and CTM policies. Compliance can impact the casino's financial performance and reputation, directly affecting their investment.
 - 2.1.6. Financial Institutions. Banks and financial partners that facilitate transactions for our online casino and require assurance that our Company follow robust AML and CTM policies. This is crucial for maintaining banking relationships and ensuring smooth financial operations.
 - 2.1.7. Legal Team. Our Legal team Responsible for advising on regulatory requirements and potential legal implications of policy breaches. They ensure that the casino's policies align with the current legal landscape and international standards.
 - 2.1.8. Third-party suppliers, that facilitate any services and products for our Company.

3. DEFINITIONS AND ABBREVIATIONS

- 3.1. **AML** – Anti-Money Laundering.
- 3.2. **CFT** – Combating the Financing of Terrorism.
- 3.3. **Company** – Interseal B.V., a legal entity validly registered and existing under the laws of Curacao, identification number: 163945, adress: Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Cente, Curasao.
- 3.4. **CDD** – Customer Due Diligence.
- 3.5. **GCB** – Gaming Control Board of Curacao.
- 3.6. **POCA** – The Proceeds of Crime Act.
- 3.7. **OFAC** – Office of Foreign Assets Control.
- 3.8. **SDN** – Specially Designated Nationals and Blocked Persons list ("SDN List").
- 3.9. **FATF** – Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
- 3.10. **NAF** – Netherlands Antillean guilder, the currency of Curaçao.
- 3.11. **NOIS** – National Ordinance on Identification when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2010, no. 40 as last amended by N.G. 2015, no. 69).
- 3.12. **NORUT** – National Ordinance on the Reporting of Unusual Transactions (Lands- verordening Melding Ongebruikelijke Transacties, N.G. 2010, no. 41 as last amended by N.G. 2015, no. 68).
- 3.13. **FIU** – The Financial Intelligence Unit Curacao.
- 3.14. **PEP** – an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:

heads of state, heads of government, ministers and deputy or assistant ministers; members of parliament or of similar legislative bodies; members of the governing bodies of political parties;

members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; members of courts of auditors or of the boards of central banks; ambassadors, chargés d'affaires and high-ranking officers in armed forces;

members of the administrative, management or supervisory bodies of state-owned enterprises; directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed previously:

family members of the individuals listed previously, including spouse, partner, children and their spouses or partners, and parents;

known close associates of the individuals listed previously, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.
- 3.15. **Gambling or Gambling Game** — any online game posted on the Website that means playing a game of chance for a Prize. Game of chance includes (i) a game that involves both an element of chance and an element of skill, (ii) a game that involves an element of chance that can be eliminated by superlative skill, (iii) a game that is presented as involving an element of chance but does not include a sport.

- 3.16. **Reporting Form** – the standard form, issued by the FIU for the purpose of recording the information regarding an unusual transaction.
- 3.17. **Customer** — an individual, who uses the Website and/or familiarizes himself with the provisions of the Website, these Policy and the provisions of other documents, and intends to register on the Website to participate in Gambling (acquire a Player status).
- 3.18. **Third Parties** — any individuals and/or legal entities other than the User and/or the Player, in particular, but not exclusively: family members, spouses, friends, partners, counterparties, creditors, service providers, agents, etc.
- 3.19. **Website** — the official websites of the Company, on which Customer may play the Gambling Games.
- 3.20. In this Policy singular include the plural, and the plural include singular in cases of a need for interpretation.

POLICY IMPLEMENTATION

4. BUSINESS RISK ASSESSMENT

- 4.1. Some products or services are inherently riskier than others and are therefore more attractive to criminals, for example – online gambling. These include products or services which are identified as being more vulnerable to criminal exploitation, such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by our Company of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:
- 4.1.1. Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- 4.1.2. Anonymous payment methods, such as pre-paid cards and virtual assets;
- 4.1.3. Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or after minimal play;
- 4.1.4. Peer to peer gaming;
- 4.1.5. The use by Customer of accounts held or cards issued in the name of third parties;
- 4.1.6. The transfer of funds from one gaming account to another;
- 4.1.7. Types of financial services (credit/marker, currency exchange, check cashing);
- 4.1.8. Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- 4.1.9. Changes to financial institution accounts to fund casino account;
- 4.1.10. Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- 4.1.11. Using cash to fund a pre-paid card poses similar risks as cash;
- 4.1.12. Games involving multiple operators (Poker on platforms shared by multiple operators);
- 4.1.13. Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Company. This may be useful for dishonest customers who wish to disguise their gambling;
- 4.1.14. Use of large or frequent transactions with complex layering to obscure origin;
- 4.1.15. Features allowing anonymous or unverified gaming accounts;

- 4.1.16. Inconsistent or suspicious betting patterns or transactions;
- 4.1.17. Use of crypto-currency or other digital payment methods for transactions
- 4.2. Distribution channels risk. The channels through which a Company establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:
 - 4.2.1. Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
 - 4.2.2. While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless we adopt technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
 - 4.2.3. Where there is the involvement of a third party in the interactions between the Customer and our Company, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.
- 4.3. During the Due Diligence, the Company may identify the:
 - 4.3.1. Multiple gambling accounts or wallets – Customers may open multiple accounts or wallets with an operator in order to obscure their spending levels or to avoid threshold checks.
 - 4.3.2. Changes to bank accounts – Customers may hold several bank accounts and regularly change the bank account they use for the remote Gambling.
 - 4.3.3. Identity fraud – details of bank accounts may be stolen and used on remote gambling websites, or stolen identities may be used to open bank accounts or remote Gambling accounts.
 - 4.3.4. Pre-paid cards – these cards pose the same risks as cash, as the Company normally cannot perform the same level of checks on the cards as they can on bank accounts.
 - 4.3.5. e-wallets – some e-wallets accept cash on deposit or cryptocurrencies, which pose a higher risk, and some Customers may use e-wallets to disguise their gambling.
 - 4.3.6. Gambling Games involving multiple operators – for example, poker games often take place on platforms shared by a number of remote gambling operators, which can facilitate money laundering by Customers, such as chip dumping.
- 4.4. Deciding that a Customer presents a higher risk of money laundering or terrorist financing does not automatically mean that the person is a criminal, money launderer or terrorist financier. Similarly, identifying a Customer as presenting a low risk of money laundering or terrorist financing does not mean that the Customer is definitely not laundering money or engaging in criminal spend. Employees therefore need to remain vigilant and use their experience and common sense in applying the Company risk-based criteria and rules, seeking guidance from their nominated officer as appropriate.
- 4.5. Many Customers carry a lower money laundering or terrorist financing risk. These might include Customers who are regularly employed or who have a regular source of income from a known source which supports the activity being undertaken. This applies equally to pensioners, benefit recipients, or to those whose income originates from their partner's employment or income.
- 4.6. Where a Customer is assessed as presenting higher risk, additional information in respect of that Customer should be collected. This will help the Company to judge whether the higher risk that the Customer is perceived to present is likely to materialize, and provide grounds for proportionate and recorded decisions. Such additional information should include an understanding of where the Customer's funds and wealth have come from.

- 4.7. Our Company also revise the business risk assessment whenever there are changes to the environment within which they are operating and within their business activities, such as introduction of new payment methods, new markets, new games or regulatory changes.
- 4.8. Transaction risk including means of payment means that the Company may consider operational aspects (products, services, games, accounts and account activities) that can be used to facilitate money laundering and terrorist financing.
- 4.9. How our Company may prevent these risks? Categorize risks as low, medium, or high based on:
 - 4.9.1. The volume and size of transactions.
 - 4.9.2. The complexity and opacity of customer pathways.
 - 4.9.3. The geographic and industry-specific vulnerabilities.
 - 4.9.4. Effectiveness of existing controls.
- 4.10. To help with categorization, our Company review current measures such as:
 - 4.10.1. Customer identity verification (KYC).
 - 4.10.2. Ongoing transaction monitoring.
 - 4.10.3. Suspicious activity and transaction reporting.
 - 4.10.4. Staff training on ML/TF risks.
 - 4.10.5. Identify gaps where controls may be insufficient or require enhancement.
- 4.11. In addition, our Company uses Risk Mitigation Strategies, such as:
 - 4.11.1. Implement enhanced due diligence for high-risk customers, products, and transactions.
 - 4.11.2. Use advanced analytics and AI tools for transaction monitoring.
 - 4.11.3. Set clear thresholds and alerts for suspicious activities.
 - 4.11.4. Regularly update the risk assessment to reflect changing threats and business operations.
 - 4.11.5. Strengthen policies on customer onboarding and ongoing monitoring.
 - 4.11.6. Document findings, risk levels, and control effectiveness.
 - 4.11.7. Establish a reporting framework for suspicious activities.
 - 4.11.8. Promptly report identified ML/TF risks and suspicious activities to relevant authorities.
 - 4.11.9. Schedule regular reviews of the risk assessment.
 - 4.11.10. Adapt policies and controls based on new typologies, regulations, or operational changes.
 - 4.11.11. Train staff regularly on emerging ML/TF risks and mitigation techniques.

5. CUSTOMER RISK ASSESSMENT

- 5.1. Customer risks mean, that determining the potential money laundering and terrorist financing risks posed by a Customer, or category of Customers, is critical to the development and implementation of an overall risk-based framework. Based on the criteria specified herein, the Company may seek to determine whether a particular Customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment.
- 5.2. Customer risk is the risk of ML/TF that arises from maintaining relations with a given person. An assessment of

the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of Customers whose activities may indicate a higher risk include:

- 5.2.1. Customers who have multiple sources of income;
- 5.2.2. Customers with irregular income streams;
- 5.2.3. PEPs;
- 5.2.4. High spenders (money can be derived from illegal activities);
- 5.2.5. Disproportionate spenders (inconsistent with our Company's information about the source of wealth or income);
- 5.2.6. Improper use of third parties, criminals use third parties to gamble and break up large amounts of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- 5.2.7. Customers using multiple casino player rating accounts to hinder a casino to track their gambling activities;
- 5.3. Our Company sets a value which represents the upper value of a typical transactions. A Customer having a single source of regular income will pose a lesser risk of ML/TF than a Customer who has multiple sources of income or irregular income streams.

6. CUSTOMER ACCEPTANCE POLICY

- 6.1. The Customer Acceptance Policy specifies the criteria used to decide whether a Customer can be approved to open an account or if further scrutiny is needed due to a higher level of risk.
- 6.2. Prohibited Customers include:
 - 6.2.1. Individuals who refuse to provide necessary information or documentation, do not supply sufficient information, fail to disclose their identity, or where KYC processes cannot be carried out.
 - 6.2.2. Individuals who provide False Information.
 - 6.2.3. Individuals who use aliases, hide their real names, or give false information to mask their identity.
 - 6.2.4. Individuals who appear on sanction lists issued by the Money Laundering Officer (MLRO) or international organizations.
 - 6.2.5. Individuals suspected of using the Company for money laundering, terrorist financing, or financing the proliferation of weapons of mass destruction.
 - 6.2.6. Individuals under the legal age of 18 (or the age of majority in their jurisdiction). Anyone under eighteen cannot be registered as a Player, and any deposits or winnings from such individuals will be forfeited to the Regulatory Authority.
 - 6.2.7. Politically Exposed Persons (PEPs). These are individuals with prominent political roles or high-profile public functions, presenting a greater risk of involvement in money laundering or terrorist financing due to their positions.
 - 6.2.8. It is forbidden to use our services by Curacao residents, therefore, Clients cannot visit our Website from Curacao.

7. CUSTOMER DUE DILIGENCE

- 7.1. The Company is entitled to conduct the Customer Due Diligence measures when:
 - 7.1.1. Establishing business relations.

- 7.1.2. Carrying out occasional transactions on and/or above the monetary equivalent of EUR 2 200, or the equivalent of Naf. 4 000 in currency available on the Website (Enhanced due diligence shall be performed in this case).
- 7.1.3. There is a suspicion of money laundering or terrorist financing.
- 7.1.4. The Company has doubts about the veracity or adequacy of previously obtained Customer identification data.
- 7.2. The Company is entitled to verify the identity of the Clients using reliable and independent sources. The Company shall see to it that the identity data is correct. When it turns out that these data are no longer in accordance with reality, the Company is entitled to adjust these modified identity data.
- 7.3. The Company conducts the Customer Due Diligence:
 - 7.3.1. To identify the Customer and verify that Customer's identity using reliable, independent source documents, data or information.
 - 7.3.2. To identify the beneficial owner and take reasonable measures to verify the identity of the beneficial owner.
 - 7.3.3. To understand and, as appropriate, to obtain information on the purpose and intended nature of the business relationship.
 - 7.3.4. When identifying the Customer, at a minimum the following information must be collected: full name; permanent residential address; date of birth; place of birth; nationality; identity number.
- 7.4. To carry out the Customer Due Diligence the Company is entitled to receive from the Client-individual the following documents: (i) an ID card, or (ii) a passport, or (iii) a driver's license.
- 7.5. In addition, the Company is entitled to receive from the Client the following documents (in case of Enhanced Due Diligence): (i) a birth certificate, (ii) residence permit, (iii) tax bills, (iv) utility bills, (v) bank, building society or credit union statement or passbook containing current address.
- 7.6. The Company is entitled to verify whether the individual is acting for himself or for a third party. If the individual acts for a third party, the Company is entitled to establish the identity of that third party with the help of the documents submitted by the individual. If the third-party acts for another third party, the Company is entitled to establish the identity of that other third party, etc.
- 7.7. If the Company knows or should reasonably suspect that the individual is not acting for himself, the Company is entitled to take reasonable measures in order to trace the identity of the Client for whom he is acting and in the event of representing a Client by a third party of that representative.
- 7.8. Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.
- 7.9. The Company is entitled to record the following data in such a manner that they are accessible:
 - 7.9.1. The name, the address, the identification information from an (i) ID card, or (ii) a passport, or (iii) a driver's license, the residence or place of establishment of the Client and the ultimate interested party, if there is any, and/or the person in whose name a payment or transaction is made, and also of their representatives.
 - 7.9.2. The nature, the number and the date and place of issue of the document with the help of which the identification has taken place.
 - 7.9.3. Current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, family circumstances.
 - 7.9.4. Phone number, Email address, mailing address, other contacts.
- 7.10. The Company is entitled to use reliable electronic systems to help with verification. Some of these systems also have the advantage of assisting with the identification of PEPs. The amount of electronic information available about individuals will vary, depending on the extent of their electronic 'footprint'. Electronic data

sources can provide a wide range of confirmatory material without necessarily requiring the Customer to produce documents. Electronic sources can be a convenient method of verification. They can be used either as the sole method of verification, or in combination with traditional document checks, on a risk basis. For an electronic check to provide satisfactory evidence of identity on its own it should (i) use data from multiple sources, across time, and (ii) incorporate qualitative checks that assess the strength of the information supplied.

- 7.11. The Company is entitled to obtain or to view the original documents and ensuring that they are valid and genuine, by comparing them to published, authoritative guidance that outlines security features (which protect against forgeries). In addition, the Company is entitled to compare the person presenting the document, or making the document available, to the document itself (for example, photograph comparison or comparison of information).
- 7.12. If the Company has any doubts on the provided documents, the Company is entitled to conduct electronic verification through a scheme which properly establishes the customer's identity, not just that the customer exists and to obtain information from another person in the regulated sector (for example, from banks), that can be used in conjunction with other documents and information to prove a customer's legitimacy over time, or positive or negative information.
- 7.13. Before opening an account, and on an ongoing basis, the Company will check to ensure that a Customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (See the OFAC website for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, we will consult them on a regular basis and subscribe to receive any available updates when they occur. With respect to the SDN list, we may also access that list through various software programs to ensure speed and accuracy. See also OFAC's Sanctions List Search tool, which screens names against the SDN list and other sanctions lists administered by OFAC. The Company will also review existing accounts against the SDN list and listings of current sanctions and embargoes when they are updated and [he or she] will document the review.
- 7.14. The Company does not permit accounts to be opened by, or to make any deposits nor used from, customers located or domiciled in Afghanistan, American Samoa, Aruba, Cyprus, Curacao, Democratic People's Republic of Korea (North Korea), Ethiopia, Guyana, Guam, Iraq, Iran, Laos, Samoa, Saudi Arabia, Russia, Belarus, Saba, Serbia, Singapore, Statia, St. Maarten St. Eustatius, Syria, Sri Lanka, Uganda, United States of America, Vanuatu, Venezuela, Trinidad and Tobago, Yemen or countries that are placed by FATF to the "black list" of countries.
- 7.15. Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our Customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. The Company will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).
- 7.16. Our Company may use documents to verify Customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and Social Security number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).
- 7.17. We understand that we are not required to take steps to determine whether the document that the customer

has provided to us for identity verification has been validly issued and that we may rely on government-issued identification as verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the Customer's true identity.

- 7.18. We will verify the information within a reasonable time before the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we will, after internal consultation with the firm's AML Compliance Person, file a SAR in accordance with applicable laws and regulations.
- 7.19. The Company is entitled to engage third parties to conduct Customer Due Diligence subject to confidentiality.
- 7.20. The Client Due Diligence shall be performed till the moment of receiving all needed documents and information according to this Policy or till the moment when the Client rejects or unable to provide all needed documents and information for more than 2 weeks from the request date. When the Client rejects or unable to provide all needed documents and information for more than 2 weeks from the request date the AML specialist shall record the suspicious and shall execute the measures that are provided in this Policy.
- 7.21. In case the Responsible person after initial stage didn't reveal the risks above, it is possible to provide a Simplified Due Diligence (SDD) that include a basic identity check for clients considered to have a very low risk of involvement in money laundering, terrorist financing, or other financial crimes. It is specifically designed for situations where the threat of such illegal activities is minimal. The applicability of SDD is determined through a preliminary risk assessment, which considers factors such as the nature of the customer's business activities, geographical location, and the transparency of their financial transactions. Customers who qualify for SDD typically include those with a clear and straightforward financial profile, for whom extensive verification processes would not proportionately enhance risk management.
- 7.22. SDD may only be applied to customers assessed as low-risk following a documented risk assessment, such as individuals with a single, verifiable income source from a regulated jurisdiction. SDD is prohibited if there is any suspicion of money laundering or terrorist financing, even in low-risk cases.
- 7.23. Our Company, directors, officers and employees are prohibited to disclose the fact that a Customer is being reported to the FIU. A risk exists that Customers could be unintentionally tipped off when the Company is seeking to perform its CDD obligations in these circumstances. Therefore, if the Company has a suspicion that transactions relate to ML or TF, it should take into account the risk of tipping-off when performing the CDD process. If our Company reasonably believes that performing the CDD process will tip-off the Customer, it may choose not to pursue that process, and should file a report to the FIU.
- 7.24. Verification is carried out by the Company to determine to its own satisfaction that the Customer is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is legitimate and that it has not been stolen from the true owner. If our Company obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly when the type of document is unfamiliar.

8. COUNTER-PARTY DUE DILIGENCE

- 8.1. If the Customer is a legal person or a corporation, the identity shall be established with the help of a certified extract from the register of the Chamber of Commerce and Industry, or a similar institution, in the country of establishment, or with the help of an identification document to be drawn up by the Service Provider. The extract or the identification document must contain at least the data to be determined by the Minister.

- 8.2. The Company is entitled to conduct the following measures:
- 8.2.1. Basic Check – Entails database, litigation and regulatory checks to highlight any known non-compliance or litigation issues. Also includes adverse information and known political Affiliations.
 - 8.2.2. Enhanced Check – Enhanced check can be conducted for counter-parties which carry medium to low level of risk. Includes validation of corporate/personal details and checks on the integrity, track record and reputation.
 - 8.2.3. Discreet Checks – Can be conducted for critical counter-parties, including large intermediaries, vendors handling sensitive information, third parties with suspicious record.
- 8.3. The Company is entitled to review the financial statements, statutory documents and to research any information available on the reputation and corporate governance.
- 8.4. The Company is entitled to engage third parties to conduct Counter-Party Due Diligence subject to confidentiality.
- 8.5. Our Company in also identify and verify the identity of the beneficial owner. As a general rule, our Company should make sure that Customers are registering an account to play and transact on their behalf. This is achieved by including specific wording in the terms and conditions that a registering Customer must explicitly accept, together with a declaration in the form of a tick box that a Customer is registering to play on his/her own behalf. Our Company is not expected to merely rely on said declaration, but have to ensure that their ongoing procedures allow for the detection of possible instances where the Customer is actually playing on behalf of third parties.
- 8.6. Our Company is acknowledged that in the majority of cases, we will not encounter situations involving beneficial owners. However, these situations cannot be excluded completely as our Company may be maintaining business relations with one or more Customers funded by a syndicate. In such circumstances, where the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as beneficial owners and our Company would therefore have to identify them and verify their identities.
- 8.7. One of the requirements of CDD is for subject persons to understand why a prospective business entity is seeking to acquire a specific service or product from them. This CDD measure means that during business relations our Company develop a risk profile of business entity to have sufficient information available to allow the detection of unusual activity in the course of a business relationship. Our Company collects sufficient information and, where it is necessary, documentation to establish and expected level of activity.
- 8.8. Source of wealth consists of determining the activities which generate the business entity's net worth and whether this justifies the projected and actual level of activity. As to the extent of the information that our Company collects, it is essential that this reflects the level of ML/FT risk identified through the business entity risk assessment. Where the risk is not high, a declaration from the business entity with some details (e.g. nature of employment/business, usual annual salary etc.) can be sufficient. Social media can also be used as a source of information.
- 8.9. However, where the risk of ML/FT is higher or our Company has doubts as to the veracity of the information collected, the information obtained will be substantiated by independent and reliable information and documentation. In developing a business entity's risk profile, our Company may also consider using statistical data to develop behavioral models against which to eventually gauge business activity rather than collect source of wealth information. It is important to note that the use of statistical data is incompatible with high-risk situations in which the transactional pattern will deviate from the average behavioral model. In such circumstances, our Company may collect sources of wealth information as set out above.

9. ENHANCED MONITORING AND DUE DILIGENCE

- 9.1. The Company conducts enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination. The Company is entitled to conduct Enhanced Due Diligence for high risk Customers, consistent with the risks identified when:
- 9.1.1. The Company obtains additional information on the Customer (e.g. occupation, volume and assets, information available through public databases, internet, etc.) and updating more regularly the identification data of Customer.
- 9.1.2. The Company obtains information on the source of funds or source of wealth of the Customer that was not mentioned before.
- 9.1.3. The Company obtains information that a Customer or potential Customer is a PEP, or a family member or known close associate of a PEP. In this case, before establishing the relationship with this Customer, a written official approval shall be obtained from Managing Director. Compliance Officer shall send the request to the Managing Director not later than in 5 business days after revealing a PEP, or a family member or known close associate of a PEP. The Managing Director shall send the official approve or official rejection in 5 business days after receiving an email from the MLRO. The Compliance Officer shall conduct an annual review of such relationships to reassess risk and ensure compliance with EDD measures.
- 9.1.4. The Customer provides the Company with unusual or suspicious identification documents that cannot be readily verified or are inconsistent with other statements or documents that the customer has provided or, the Customer provides information that is inconsistent with other available information about the Customer.
- 9.1.5. In any case, identified by the Company or in information provided by the GCB to the Company as one where there is a high risk of money laundering or terrorist financing.
- 9.1.6. In any business relationship with a Customer situated in a high-risk third country or in relation to any transaction in relation to which the operator is required to apply CDD measures, where either of the parties to the transaction is resident in a high-risk third country.
- 9.1.7. In any case, where the Company discovers that a Customer has provided false or stolen identification documentation or information and the operator proposes to continue to deal with the Customer
- 9.1.8. In any case, where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose.
- 9.1.9. In any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.
- 9.1.10. The Customer refuses to identify a legitimate source of funds or information is false, misleading or substantially incorrect.
- 9.1.11. The Customer is domiciled in, doing business in or regularly transacting with counterparties in a jurisdiction that is known as a bank secrecy haven, tax shelter, high-risk geographic location (e.g., known as a narcotic (drugs) producing jurisdiction, known to have ineffective AML/Combating the Financing of Terrorism systems) or conflict zone, including those with an established threat of terrorism.
- 9.1.12. The Customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- 9.1.13. The Customer's legal or mailing address is associated with multiple other accounts or businesses that do not appear related.
- 9.1.14. The Customer appears to be acting as an agent for an undisclosed principal, but is reluctant to provide

information.

- 9.1.15. The Customer's background is questionable or differs from expectations based on business activities.
- 9.1.16. The Customer's business activities are entitled with the high-risk source of wealth incomes, for example in crypto business, casino/gambling business/finance business/ manufacture of weapons business or the Customer cannot describe the source of wealth.
- 9.1.17. The Customer use a high-risk payment method – payments in crypto and/or payments from shell banks and/or payments from banks that are established or registered or in which it operates in territories with high geographical risk and/or payments from the credit/debit cards that not belong to the Customer and/or unauthorized payments and/or payments that close or exceed the limits.
- 9.1.18. The Customer may not act independently or may act in favor of any other third-party or unknown beneficiary owner.
- 9.2. During the enhanced Due Diligence, the Company is entitled to receive from the Client-individual the following documents:
 - 9.2.1. Written explanations on the source of funds or source of wealth of the Customer and the documents that may approve those explanations.
 - 9.2.2. Written explanations on the wealth and/or working capacity of the Client.
 - 9.2.3. Any documents that can prove the written explanations.
 - 9.2.4. Additional information on the intended nature of the business relationship.
 - 9.2.5. Information on the reasons for the transactions.
- 9.3. The Company is entitled to ensure that documents, data, and information collected through the Customer Due Diligence measures are kept up-to-date and relevant by undertaking reviews of existing records, particularly for higher risk categories of customers.
- 9.4. The Customer Due Diligence measures include:
 - 9.4.1. Identification process that is begins by developing an initial list of potential risks or risk factors when combating money laundering and terrorist financing. Risk factors are the specific threats or vulnerabilities that are the causes, sources or drivers of money laundering and terrorist financing risks. This list will be drawn from known or suspected threats or vulnerabilities. The identification process should be as comprehensive as possible, although newly identified or previously unidentified risks may also be considered at any stage in the process.
 - 9.4.2. Analysis process involves consideration of the nature, sources, likelihood, impact and consequences of the identified risks or risk factors. The aim of this stage is to gain a comprehensive understanding of each of the risks, as a combination of threat, vulnerability and consequence, in order to assign a relative value or importance to each of them. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk, the purpose of the risk assessment, and the information, data and resources available.
 - 9.4.3. The evaluation stage involves assessing the risks analyzed during the previous stage to determine priorities for addressing them, considering the purpose established at the beginning of the assessment process. These priorities can then contribute to development of a strategy for the mitigation of the risks.
- 9.5. Money laundering and terrorist financing risks may be measured using a number of factors. Application of risk categories to Customers and situations can provide a strategy for managing potential risks by enabling the Company to subject customers to proportionate controls and monitoring.
- 9.6. The Company is entitled to seeking additional independent, reliable sources to verify information provided or made available to the Company and taking additional measures to understand better the background,

ownership and financial situation of the customer, and other parties to the transaction. The Company taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship.

- 9.7. In the case of transactions that are complex or unusually large, or where there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose, the enhanced measures undertaken should include:
 - 9.7.1. As far as reasonably possible, examining the background and purpose of the transaction, examining the aim of business relations with the Client and nature of Client's business.
 - 9.7.2. Increasing the degree and nature of monitoring of the business relationship in which the transaction is made, to determine whether the transaction or relationship appear to be suspicious.
 - 9.7.3. The Company is entitled to engage third parties to conduct enhanced monitoring of the business relationship subject to confidentiality.
- 9.8. The Enhanced Due Diligence shall be performed till the moment of receiving all needed documents and information according to this Policy or till the moment when the Client reject or unable to provide all needed documents and information for more than 2 weeks from the request date. When the Client rejects or unable to provide all needed documents and information for more than 2 weeks from the request date the AML specialist shall record the suspicious and shall execute the measures that are provided in this Policy.

10. ONGOING DUE DILIGENCE (MONITORING)

- 10.1. To conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Customer, their business and risk profile, including, where necessary, the source of funds. The Company is entitled to continuously monitor the Customer's transactions, considering the characteristics including types of transactions listed in annex 1 to the FATF document entitled Guidance for Financial Institutions in Detecting Terrorist Financing.
- 10.2. The Company is entitled to conduct the Ongoing Due Diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Customer, their risk profile, including where necessary the source of funds.
- 10.3. In order to be able to detect Customer activity that may be suspicious, it is necessary to monitor all transactions or activity. The monitoring of Customer activity should be carried out using the risk-based approach. Higher risk customers should be subjected to a frequency and depth of scrutiny greater than may be appropriate for lower risk Customers. The Company is aware that the level of risk attributed to Customers may not correspond to their commercial value to the business.
- 10.4. Where, through their Customer profile or known pattern of Gambling activity, the Customer appears to pose a risk of actual or potential money laundering, the Company is monitoring the gambling activity of the Customer and consider whether further due diligence measures are required. This should include a decision about whether a defense (appropriate consent) should be sought for future transactions (on a transaction by transaction basis), or whether the business relationship with the customer should be terminated where the risk of breaches of POCA are too high.
- 10.5. The Company is ensuring that the arrangements that they have in place to monitor Customers and the accounts they hold across outlets, products and platforms (remote and non-remote) are sufficient to manage the risks that the Company is exposed to. This should include the monitoring of account deposits and withdrawals.

- 10.6. If the Customer's patterns of gambling lead to an increasing level of suspicion of money laundering, or to actual knowledge of money laundering, the Company may consider whether it wish to allow the Customer to continue using the Website.
- 10.7. Transaction monitoring is executed to prevent involvement of our Company with ML/TF and to safeguard the reputation of the Company. While performing ongoing scrutiny of transactions our Company notices that a Customer's transactions are not consistent with what it know or expected from the Customer. In this case, our Company may question this unusual activity and, where necessary, establish the source of the funds used for these transactions. Source of funds refers to how the funds for a particular transaction were obtained by the Customer. The reason for the above inconsistency may be deviation, amongst others, from the source of funds or average profile or accountancy noted to date). Our aim is to understand what the reason for this deviation is and obtain sufficient information and documentation regarding the transaction. This is also one of the situations in which the risk profile of the customer may have to be revised. After receiving this information Our Company wii decide whether the transaction is an unusual transaction and need to be reported to the FIU.
- 10.8. During the Ongoing Due Diligence, a transaction may be considered as unusual if:
- 10.8.1. A transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose, or
- 10.8.2. Other activity or situation that the Company regards as particularly likely, by its nature, to be related to money laundering, terrorist financing or proliferation financing.
- 10.8.3. The Customer transacts with significant amounts of money.
- 10.8.4. The Customer transacts with multiple remote gambling operators, particularly where this occurs across multiple geographical areas.
- 10.8.5. The Customer seemingly breaks funds transfers into smaller transfers to avoid raising attention to a larger funds transfer. The smaller funds transfers do not appear to be based on payroll cycles, retirement needs, or other legitimate regular deposit and withdrawal strategies.
- 10.8.6. Payments are made by third party check or money transfer from a source that has no apparent connection to the Customer.
- 10.8.7. Wire transfers are made to or from financial secrecy havens, tax havens, high-risk geographic locations or conflict zones, including those with an established presence of terrorism.
- 10.8.8. The customer engages in transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g., countries designated by national authorities, such as FATF, as non-cooperative countries and territories).
- 10.8.9. The parties to the transaction (e.g., originator or beneficiary) are from countries that are known to support terrorist activities and organizations.
- 10.8.10. A dormant account suddenly becomes active without a plausible explanation (e.g., large deposits that are suddenly wired out).
- 10.9. The Company providing scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the Company's knowledge of the Customer, the Customer's business and risk profile. The Company undertaking reviews of existing records and keeping the documents or information obtained for the purpose of applying CDD measures up-to-date.
- 10.10. The Company is entitled to engage third parties to conduct enhanced monitoring of the business relationship subject to confidentiality.
- 10.11. The Ongoing Due Diligence shall be performed on the regular basis.

11. RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE

- 11.1. Our Company may rely on third parties when performing elements of the CDD measures, provided that the criteria mentioned in this Policy are met. The third party should be subject to CDD and record-keeping requirements of the Company. The third party will have an existing business relationship with the Customer, which is independent from the relationship to be formed by the Customer with the relying institution (our Company). Where such reliance is permitted, the ultimate responsibilities for CDD measures remain with the Company relying on the third party. In this case, our Company should have an agreement with the third party being relied upon that copies of identification data or other relevant documentation relating to CDD requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Our Company, however, remains responsible for the carrying out of a Customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring.

12. RISK PROFILES

- 12.1. Our Company uses the Risk-based Approach. By adopting the Risk-based Approach, it is possible for our Company to ensure that measures to prevent or mitigate money laundering, financing of terrorism and proliferation of weapons are commensurate with the risks identified. That means the higher the risk, the more measures our Company should take to mitigate the risk. Where the risks are higher enhanced measures must be taken. Where the risks are lower it may take simplified measures, provided that this is consistent financing of terrorism risks.
- 12.2. Our Company can also use data collected over a period of time by the Company itself, which allows us to create the profile of an average Customer. Our Company should therefore only use this specific alternative where their customer-base is wide enough to allow the creation of an average profile.
- 12.3. By applying the Risk-based Approach our Company is:
- 12.3.1. Assess the risks that money laundering or terrorist financing may occur within its organization beforehand;
 - 12.3.2. Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
 - 12.3.3. Monitor and improve the effective operation of these policies, procedures and controls;
- 12.4. Document its risk assessments, including everything that has been done and the reason for this. Our Company analyzing the documents and information to identify the (i) country or geographic risks, (ii) customer risks, (iii) transaction risks, (iv) products and services offered, (v) delivery channels.
- 12.5. Country and geographic risks mean, that some countries pose an inherently higher money laundering and terrorist financing risk than others. In addition to considering their own experiences, our Company may consider a variety of other credible sources of information identifying countries with risk factors in order to determine that a country and customers from that country pose a higher risk. Our Company may wish to assess information available from FATF and non-governmental organizations which can provide a useful guide to perceptions relating to corruption in the majority of countries. Customers that are associated with higher risk countries, as a result of their citizenship, country of business or country of residence may present a higher money laundering and terrorist financing risk, considering all other relevant factors. Our Company's employees may check the Customer location because of the additional risks which arise from cross-border operations. The country or geographic risk can also be considered in conjunction with the customer risk.
- 12.6. The geographical risk is the risk posed to our Company by the geographical location of the Customer and the

source of wealth of the business relationship. The nationality, residence and place of birth of the Customer have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered as high risk. It is advisable to take into account a variety of sources of information produced by the FATF and well-known non-governmental well-known bodies. Some sources to use are:

- 12.6.1. Countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- 12.6.2. Countries on the FATF list of Jurisdictions under Increased Monitoring;
- 12.6.3. Countries on the CFATF Public Statement;
- 12.6.4. Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- 12.6.5. Countries on the European Commission's list of third countries having strategic deficiencies in the AML/CFT regime;
- 12.6.6. Countries sanctioned by the OFAC;
- 12.6.7. Countries identified by credible sources as providing funding or support for terrorist activities or having terrorist organizations operating within them;
- 12.6.8. Countries on the Corruption Perception Index compiled by Transparency International.
- 12.7. Our Company has a list of countries that are considered as high risk and of those that are considered low risk (the list is placed in the Website Policy and updated regularly).
- 12.8. Industry-Specific Risk Indicators. The Company shall monitor for red flags specific to online gambling, including but not limited to:
 - 12.8.1. Customers frequently altering betting patterns or using multiple accounts to evade detection.
 - 12.8.2. Deposits followed by minimal gambling activity and rapid withdrawals.
 - 12.8.3. Use of "chip dumping" or collusion in peer-to-peer games.

13. CRYPTOCURRENCY

- 13.1. Virtual Assets and Cryptocurrencies:
- 13.2. Customers using cryptocurrencies for deposits or withdrawals shall undergo Enhanced Due Diligence, including verification of the source of funds via blockchain analysis where possible.
- 13.3. The Company shall monitor for suspicious patterns, such as rapid conversion of cryptocurrencies to fiat currency with minimal gambling activity, and report such transactions to the FIU as required.

14. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE. TERMINATION OF BUSINESS RELATIONSHIP AND ASSETS FREEZE

- 14.1. To avoid potentially committing one of the principal money laundering offences, The Company may to consider ending the business relationship with a Customer in the following circumstances:
 - 14.1.1. Where it is known that the Customer is attempting to use the Gambling Games to launder criminal proceeds or for criminal spend.

- 14.1.2. Where the risk of breaches to POCA are considered by the Company to be too high.
- 14.1.3. Where the Customer's Gambling activity leads to an increasing level of suspicion, or actual knowledge of, money laundering.
- 14.1.4. Where the Customer is proven to a reasonable degree of confidence to not be the identity they claim to be.
- 14.1.5. When the Company is unable to apply the CDD measures.
- 14.1.6. If the requested information and documentation is not received within 30 days from the moment the equivalent of Naf. 4,000 thresholds were reached.
- 14.2. Our Company shall terminate the relationship with the Customer and report to the FIU if a presumption of money laundering or terrorist financing exists. If no presumption of money laundering exists, the funds should be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, internal procedures should indicate whether the funds are blocked or not. Consideration should be given to the fact that by blocking the account, the customer may be tipped off.
- 14.3. Targeted financial sanctions require us to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities, therefore, all natural and legal persons in Curaçao are required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities. This is to comply with United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. EU sanctions are binding for Curaçao on the basis of the Kingdom Sanctions Act.
- 14.4. Our Company implements a mechanism to check the sanction status of a withdrawing participant so that a sanctioned person or organization cannot remove money from the Account that should be frozen. In such cases, our Compliance Officer will fill a report with the FIU and our Company will take the Process for the freezing of resources (assets).
- 14.5. Fund Handling Upon Termination: When terminating a relationship due to suspicion of money laundering or terrorist financing, the Company shall freeze the customer's funds and consult the FIU before any disbursement. In non-suspicious cases, funds shall be returned to the originating account within 14 calendar days, subject to risk assessment.

15. REPORTING OF SUSPICIONS

- 15.1. If the Company suspects or has reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts, or terrorist organizations, it shall promptly report its suspicion to the FIU in accordance with art. 11 of the NORUT.
- 15.2. By virtue of article 11 of the NORUT, the Company shall report any unusual transaction or any intended unusual transaction to the FIU without delay. Unusual transactions shall be reported in compliance with the NORUT.
- 15.3. The following transactions or intended transactions are deemed unusual:
 - 15.3.1. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance
 - 15.3.2. Transactions which in connection with money laundering or terrorism financing are reported to the police authorities or to the following department of justice.
 - 15.3.3. We may file a voluntary FIU for any suspicious transaction that we believe is relevant to the possible violation

of any law or regulation but that is not required to be reported by us under the FIU rule. It is our policy that all FIU will be reported regularly to the Board of Directors and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the FIU.

- 15.3.4. We will retain copies of any FIU filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the forms. We will identify and maintain supporting documentation and make such information available to any appropriate law enforcement agencies, state regulators upon request.

16. RECORDING AND REPOTING

- 16.1. The Company is recording each unusual transaction individually on a reporting Form. Individual reporting forms are numbered sequentially. Any Reporting Form that is voided shall be retained by the Company.
- 16.2. The Company is maintaining records, containing the information and documentation necessary to decide whether the objective of the CDD measures referred to in this policy was met, and to establish the background and purpose of transactions, for at least five years after the business relationship is ended, or after the date of the occasional transaction.
- 16.3. Each report about an unusual transaction will include at least the following information:
 - 16.3.1. The identity of the Client.
 - 16.3.2. Nature and number of the identification document of the Client.
 - 16.3.3. The nature, date, time and place of transaction.
 - 16.3.4. The amount, destination and origin of the funds, securities, precious metals, or other values involved in the transaction
 - 16.3.5. The circumstances that identified the transaction as unusual.
- 16.4. The Compliance Officer signs the reporting form if it is submitted manually.
- 16.5. The senior management (director, executive director, CEO, etc.) is entitled to sign the reporting form with the verbal consent of the Compliance Officer.
- 16.6. By virtue of article 11 of the NORUT, our Company reports unusual transaction or any intended unusual transaction to the FIU without delay. In order to do this, it should have clear procedures for internal and external reporting of unusual transactions in place. These should be communicated to its personnel. All unusual individual transactions or series of transactions, as mentioned in Policy Indicators Unusual Transactions, must be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting.
- 16.7. The Company may use an electronic system approved by the FIU for this purpose, or submit a paper copy of the reporting form. Submission of paper forms shall not be done by fax for the purpose of data security. In either case, our Company will retain a copy of the reporting form for its own records, which are available to GCB agents upon request.
- 16.8. The Company providing information or documentation on money laundering and terrorist financing policies and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year.
- 16.9. The Company making the following documents and information readily available:
 - 16.9.1. Its written and approved policy and procedures on money laundering and terrorist financing prevention.
 - 16.9.2. The name of each Compliance Officer responsible for the Company's overall money laundering and terrorist

financing deterrence and detection procedures and her/his designated job description.

- 16.9.3. Records of reported unusual transactions
- 16.9.4. Records on unusual transactions which required closer investigations.
- 16.9.5. The completed source of funds declaration.
- 16.9.6. Schedule of the training provided to our personnel regarding money laundering and terrorist financing.
- 16.9.7. The assessment report on the Company's policies and procedures on money laundering and terrorist financing by the internal audit department or the Company's external auditor.
- 16.9.8. Required copies of identification documents.
- 16.10. The listing above is not limitative and does not exclude the Company from providing additional information and documentation if the GCB so requests.
- 16.11. In addition, the Company maintain a record in writing of its (i) policies, procedures and controls, (ii) any changes to those policies, procedures and controls, (iii) the steps the Company have taken to communicate the policies, procedures and controls or any changes to them, within the Company's business.
- 16.12. The Company may share information with financial institutions or governmental authorities regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. Before we share information with financial institutions or governmental authorities, we will take reasonable steps to verify that the financial institutions or governmental authorities are entitled to receive that information according to the legislation.
- 16.13. We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information.
- 16.14. We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:
 - 16.14.1. Identifying and, where appropriate, reporting on money laundering or terrorist activities;
 - 16.14.2. Determining whether to establish or maintain an account, or to engage in a transaction; or
 - 16.14.3. Assisting the financial institution or gambling operator in complying with performing such activities.
- 16.15. If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, we will reject the transaction and/or block the customer's assets and file a blocked asset and/or rejected transaction form with OFAC within 10 days.
- 16.16. Our Company is not only required to adhere to the stipulations of the National Ordinance for Identification of Services but are also required to detect and report either intended or completed unusual transactions. Our Company has adequate procedures in place that cover the following (i) the recognition of unusual transactions, (ii) the documentation of unusual transactions, and (iii) the reporting of unusual transactions.
- 16.17. An unusual transaction is a transaction inconsistent with the Customer's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the Customer. The purpose of collecting Customer information is to provide the Company with documentation to assess the risk that may be associated with the Customer and to build a Customer profile to assess how the Customer is going to act within the framework of the business relationship. Based on the NORUT legislation, objective and subjective indicators have been established by means of which our Company should assess whether a Customer's transaction qualifies as an unusual transaction.
- 16.18. Our management provides our staff with specific guidance and training in recognizing and adequately

documenting unusual transactions. All these unusual transactions must be reported to the Compliance Officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements. The Compliance Officer must keep an adequate filing system of these records. If internally reported transactions are not reported to the FIU by the Company, the reasons therefore shall be adequately documented and signed off by the Compliance Officer and/or management.

- 16.19. In order to implement FAT recommendation, Our Company pays special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The following transactions or intended transactions are deemed unusual:
- 16.19.1. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- 16.19.2. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- 16.19.3. Transactions in the amount of equivalent of NAf. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to: A cashless transaction in the amount of equivalent of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the Customer. Accepting or releasing a deposit in the amount of equivalent of NAf. 5,000 or more at the request of the Customer.
- 16.20. A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000 or more and is considered per gaming day.
- 16.21. Our Company registered with the FIU and to obtain access to the goAML reporting portal after validation by the FIU. The FIU allows bulk reporting, therefore our account manager at the FIU should be contacted in order for the FIU to determine if the operator qualifies for this service.

17. COOPERATION WITH AUTHORITIES

- 17.1. The Company shall cooperate fully with law enforcement and regulatory authorities, providing requested information within 5 business days unless otherwise specified.
- 17.2. The Compliance Officer shall serve as the primary point of contact for such inquiries.

18. OTHER MESURES

- 18.1. Our Company shall assess the Technological Development Risk. This risk arises from various sources, including legacy systems, cyber-attacks, software malfunctions, hardware failures, and data integrity issues, all of which directly impact business operations and strategic outcomes. Effective technology risk management integrates the identification, assessment, and prioritization of these risks, employing strategic mitigation and response strategies.
- 18.2. Our Company maintains appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It should identify and assess the money laundering or terrorist financing risks that may arise whenever:
- 18.2.1. A new product has been developed;
- 18.2.2. A new business practice emerges;
- 18.2.3. A new delivery mechanism is becoming available;

- 18.2.4. New or developing technology is used for both new and pre-existing products.
- 18.3. In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments must be documented. Where risks are identified, measures must be taken to mitigate these risks.
- 18.4. The Company shall conduct a comprehensive review of its risk assessment at least annually or upon significant changes, such as new products, payment methods, or regulatory updates.
- 18.5. Where the Company is unable to complete or apply the required CDD measures in relation to a particular Customer at the point the CDD threshold for transactions is reached, and are accordingly required to cease transactions or terminate the business relationship with the Customer, the Company may adopt the following procedure:
- 18.6. At the point where the threshold is reached, the Company may put all funds owed to the Customer into an account (or equivalent) from which no withdrawals can be made.
- 18.7. Further deposits can be made to that account as long as they are also locked into it until CDD is completed.
- 18.8. Bets can be made from the account, again providing any winnings are locked until CDD is completed
- 18.9. Once CDD is completed, the account can be unlocked and business continue as normal.
- 18.10. If CDD cannot be completed, then the Company shall terminate the existing business relationship with the Customer
- 18.11. If funds are to be repaid, then the amount repaid should consist of all funds owed to the customer at the point that the threshold was reached, plus all deposits made at that point and thereafter.
- 18.12. Funds should be refunded back to the originating account, and there should be appropriate risk mitigation. Where it is suspected that the funds are the proceeds of crime, we will submit FUI or seek a defense (appropriate consent) before refunding any of the funds.
- 18.13. There should be ongoing monitoring of the account and, if necessary, reporting of findings via relevant fraud monitoring services in the public and private sector.
- 18.14. The Company may suspend, block or close the Customer's personal account and retain all funds, if required by anti-money laundering legislation. The Company reserves the right to use additional procedures and tools to verify compliance of all operations.
- 18.15. Automated Transaction Monitoring: The Company shall utilize automated systems to monitor transactions, with predefined thresholds (e.g., transactions exceeding NAF 10,000 or unusual frequency) triggering manual review by the Compliance Officer.

19. THE COMPLIANCE OFFICER (MONEY LAUNDERING REPORTING OFFICER (MLRO): APPOINTMENT AND RESPONSIBILITIES.

- 19.1. The Company assigning a Compliance Officer (or Money Laundering Reporting Officer (MLRO)) within its organization, who shall monitor compliance with Curaçao AML/CFT laws and regulations as well as with the our internal policies and procedures, as referred to the NOIS.
- 19.2. The Compliance Officer is holding a position within the Company organization at least middle managerial level. The Compliance Officer may be charged with additional management responsibilities.
- 19.3. The Compliance Officer is independent of the Company Games Operations.

- 19.4. The Compliance Officer shall be able to carry out his/her function independently and effectively.
- 19.5. The Compliance Officer shall have timely access to customer identification data and other CDD information, transaction records, and other relevant information.
- 19.6. The Compliance Officer is responsible for the proper execution of the provisions in this regulation and the necessary training the personnel of the Company to be able to identify and report unusual transactions, which include the following activities:
 - 19.6.1. To organize training sessions for the staff on various compliance-related issues.
 - 19.6.2. To review compliance with the Company's policy and procedures.
 - 19.6.3. To analyze transactions and verify whether any are deemed unusual under the NORUT and hence subject to reporting to the FIU.
 - 19.6.4. To review all internally reported unusual transactions for their completeness and accuracy with other sources.
 - 19.6.5. To keep records of internally and externally reported unusual transactions.
 - 19.6.6. To prepare the external report of unusual transactions.
 - 19.6.7. To execute closer investigation of unusual or suspicious transactions.
 - 19.6.8. To remain informed of the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements.
 - 19.6.9. To prepare periodic information on the Company's efforts against money laundering and terrorist financing.
- 19.7. The above-mentioned responsibilities is included in the job description of each Compliance Officer. The job description is signed off on and dated by the officer, indicating her/his acceptance of the entrusted responsibilities.
- 19.8. We inform the Gaming Control Board and the FIU of the identity of the Compliance Officer and of any changes regarding this position.
- 19.9. To demonstrate compliance with the aforementioned training requirements, the Company carry out at all times maintain records that include:
 - 19.9.1. Details of the content of the training programs provided.
 - 19.9.2. The names of staff who have received the training.
 - 19.9.3. The date on which the training was delivered.
 - 19.9.4. The results of any testing carried out to measure staff understanding of the money laundering and terrorist financing requirements.
 - 19.9.5. An ongoing training plans.
- 19.10. With the Compliance Officer, the senior management is fully engaged in the processes for the Company's assessment of risks for money laundering, terrorist financing and proliferation financing, and is involved at every level of the decision making to develop the Company's policies and processes to comply with the regulations.
- 19.11. The senior management is entitled to:
 - 19.11.1. Examine and evaluate the adequacy and effectiveness of the policies, procedures and controls adopted by the operator to comply with the Regulations.
 - 19.11.2. Make recommendations in relation to those policies, procedures and controls.
 - 19.11.3. Monitor the Company's compliance with those recommendations.

20. TRAINING

- 20.1. The Company shall ensure that its employees understand the AML regulations, data protection issues, apply the operator's policies, procedures and controls, including the requirements for CDD, record keeping and SARs.
- 20.2. One of the most important controls for the prevention and detection of money laundering, terrorist financing and proliferation financing is to have employees who are alert to the risks of money laundering, terrorist financing and proliferation financing, and who are well trained in the identification of unusual activities or transactions which appear to be suspicious, as well as in the accurate verification of Customer's' identities. The effective application of even the best designed control systems can be quickly compromised if the employees applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of our AML or CTF strategy.
- 20.3. The Company should devise and implement a clear and well-articulated policy and procedure for ensuring that relevant employees are aware of their legal obligations in respect of the prevention of money laundering, terrorist financing and proliferation financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering, terrorist financing or proliferation financing. The Company should also monitor the effectiveness of such training, to ensure that all employees are trained in an appropriate and timely manner, and that the training is fit for purpose.
- 20.4. The Company taking appropriate measures so that its relevant employees, and any agents they use for the purposes of their business whose work are:
 - 20.4.1. Made aware of the law relating to money laundering, terrorist financing and proliferation financing, and to the requirements of data protection, which are relevant to the implementation of the regulations.
 - 20.4.2. Data Protection Compliance: The Company shall ensure customer data collected for AML/CTF purposes is stored securely and processed in compliance with applicable data protection laws, such as the General Data Protection Regulation (GDPR) where relevant. Data shall only be shared with authorized parties under strict confidentiality agreements.
 - 20.4.3. Regularly given training in how to recognize and deal with transactions and other activities or situations which may be related to money laundering, terrorist financing or proliferation financing.
- 20.5. The Company is maintaining a record in writing of the appropriate training measures they have taken and, in particular, of the training given to their relevant employees and to any agents they use for the purposes of their business whose work is of a kind mentioned in the following paragraph.
- 20.6. The Company's employees whose work is relevant to the Company's compliance with any requirements in the regulations, or able to contribute to (i) the identification or mitigation of the risk of money laundering, terrorist financing or proliferation financing to which the operator's business is subject, or (ii) the prevention or detection of money laundering, terrorist financing or proliferation financing in relation to the operator's business.
- 20.7. The content of any training, the regularity of training and the assessment of competence following training are matters for us to assess and decide in light of the money laundering, terrorist financing and proliferation financing risks they identify, provided the requirements of regulation are met.
- 20.8. The Company ensures that the employees are aware of and understand:
 - 20.8.1. Their responsibilities under the operator's policies and procedures for the prevention of money laundering, terrorist financing and proliferation financing.
 - 20.8.2. The Company's procedures for managing those risks.

- 20.8.3. The identity, role and responsibilities of the nominated officer, and what should be done in their absence.
- 20.8.4. The potential effect of a breach upon the operator and upon its employees.
- 20.8.5. How the Company will undertake CDD.
- 20.8.6. How the Company will track customers when CDD is not undertaken on entry to our Website.
- 20.8.7. How PEPs, family members of PEPs and known close associates of PEPs will be identified, and how to distinguish PEPs who present a relatively higher risk from those who present a relatively lower risk.
- 20.9. There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. Procedure manuals, whether paper or electronic, are useful in raising employee awareness and can supplement more dedicated forms of training, but their main purpose is generally to provide ongoing reference rather than being written as training material. Ongoing training must be given to all relevant employees at appropriate intervals. Records should be maintained to monitor who has been trained, when they receive the training, the nature of the training and the effectiveness of the training.

21. NOTIFICATIONS

- 21.1. The Company is entitled to provide notice to Customers that the Company is requesting information from them to verify their identities, as required by the legislation.
- 21.2. The Company is entitled to provide any other notices to Customer, for example – termination notice, notice of blocking of the account, warning notice, etc.
- 21.3. We will use the following method to provide notices to customers – Email notice and/or phone call and/or internal account notice and/or mail notice.

22. UPDATING POLICIES AND PROCEDURES. RELATED INFORMATION

- 22.1. The Company is required to check for amendments on Sanctions Decrees and Regulations on a regular basis and update their CDD- and AML/CFT- policies and – procedures accordingly to reflect such amendments. Such information contains lists of suspected terrorists, terrorist groups, and associated individuals and entities as mentioned in (in any case):
 - 22.1.1. The Consolidated United Nations Security Council Sanctions List.
 - 22.1.2. The Sanction Decree “Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s.” (N.G. 2015, no. 29).
 - 22.1.3. The Ministerial Regulation “Libya” (N.G. 2015, 28).
 - 22.1.4. The Sanction Decree “Islamic Republic Iran 2015” (N.G. 2015, 27).
 - 22.1.5. The Sanction Decree “Democratic People’s Republic of Korea 2015” (N.G. 2015, 30).
 - 22.1.6. The Ministerial Regulation “Yemen” (N.G. 2015, 65).
 - 22.1.7. Guidance for Financial Institutions in Detecting Terrorist Financing.
 - 22.1.8. The listing¹³ of the Office of Foreign Assets Control (OFAC).
 - 22.1.9. The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92).
 - 22.1.10. The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).
 - 22.1.11. Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions.
 - 22.1.12. (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73).

- 22.1.13. The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).
- 22.1.14. National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34).
- 22.1.15. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council.
- 22.1.16. National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nation Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28).
- 22.1.17. Kingdom Sanction Act (N.G. 2016, no. 54).
- 22.1.18. National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2).
- 22.1.19. The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92).

23. CONTACT INFORMATION

- 23.1. For any questions regarding this policy, please contact: support@pd.games or send a mail on the address: Schottegatweg Oost 10 Unit A1K 10 Unit 1-9, Bon Bini Business Center, Curaçao.

24. POLICY HISTORY

May 19, 2025	Anti-money laundering and combating the financing of terrorism policy update (Annual update)
December 02, 2024	Anti-money laundering and combating the financing of terrorism policy update (legal changes)
June 12, 2024	Anti-money laundering and combating the financing of terrorism policy update (legal changes)
May 24, 2024	Anti-money laundering and combating the financing of terrorism policy update (Annual update)
December 12, 2023	Anti-money laundering and combating the financing of terrorism policy update (legal changes)
June 20, 2023	Anti-money laundering and combating the financing of terrorism policy update (legal changes)
May 24, 2023	Initial Anti-money laundering and combating the financing of terrorism policy