

AML-CTF-CPF POLICY AND PROCEDURES

Hazarion N.V.

Contents

Contents	2
1. INTRODUCTION	4
1.1. What is Money Laundering?	4
1.2. What is the Financing of Terrorism?	4
1.3. What is Proliferation of weapons of mass destruction?	4
1.4. The Need to Combat Money Laundering, Financing of Terrorism and Proliferation of weapons of mass destruction	5
2. APPLICABLE RULES AND LEGISLATION	6
3. CUSTOMER ACCEPTANCE POLICY	8
3.1. Introduction	8
3.2. Age verification	8
3.3. Countries and territories excluded for registration	9
3.4. Accepted payment methods	11
3.5. No cash policy	12
3.6. Targeted Financial Sanctions	12
3.7. Politically Exposed Persons (PEPs)	12
3.7.1. Foreign PEPs	13
3.7.2. Domestic PEPs	14
4. BUSINESS AND CUSTOMER RISK ASSESMENT	15
4.1. Business Risk Assessment	15
4.2. Customer risk assessment	16
5. Customer Due Diligence	17
5.1. Simplified due diligence (SDD)	18
5.2. Enhanced Due Diligence	19
5.3. Accepted documents	19
5.4. Enhanced due diligence	21
5.5. Methods of verification	22
6. TECHNOLOGICAL DEVELOPMENT RISK ASSESMENT	23
7. ONGOING MONITORING	24
6.1. Scrutiny and monitoring of transactions:	24
7.1. Update the information and the documents of the clients	25
8. RECORD KEEPING PROCEDURES	27
9. REPORTING PROCEDURES AND OBLIGATIONS	28
9.1. Internal Reporting Procedures	28
9.2. External reporting procedures	30
9.3. Prohibition of Disclosure	30
10. OUTSOURCING SERVICES	32
11. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	33

11.1.	Appointment of a Money Laundering Compliance Officer	33
11.2.	Duties of the Compliance Officer	33
11.3.	Employee screening	33
11.4.	Training	34
11.5.	Independent audit function	35
12.	REGULARITY OF POLICY UPDATES	36
13.	APPENDIX 1	37
14.	APPENDIX 2	39

Version History

Ver.	Author	Date Management Approval
1.0	Hazarion N.V.	2019.03.20
2.0	Hazarion N.V.	2019.12.16
3.0	Hazarion N.V.	2020.04.20
3.1	Hazarion N.V.	2020.12.10
3.2	Hazarion N.V.	2022.08.22
3.3	Hazarion N.V.	2023.05.18
3.4	Hazarion N.V.	2024.12

1. INTRODUCTION

1.1. What is Money Laundering?

Generally, money laundering is described as the process by which the illegal nature of criminal proceeds is concealed or disguised in order to lend a legitimate appearance to such proceeds. This process is of crucial importance for criminals as it enables the perpetrators to make legitimate economic use of the criminal proceeds. When criminal activity generates substantial income, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or to the persons involved. Criminals do this by disguising the sources, changing the form or moving the funds to a place where they are less likely to attract attention.

Traditionally, three stages were identified for the process of money laundering – the placement stage, the layering stage and the integration stage.

- a) Placement: the first introduction of the cash proceeds of criminal conduct into the financial system, especially via deposit-taking institutions and, again, particularly in jurisdictions with extensive banking secrecy laws and little or no anti money laundering legislation.
- b) Layering: separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.
- c) Integration: the provision of apparent legitimacy to criminally derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the financial system.

1.2. What is the Financing of Terrorism?

Financing of terrorism is the process by which terrorist organizations or individual terrorists are financed in order to be able to carry out acts of terrorism.

The financing of terrorist activity, terrorist organizations or individual terrorists may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Funds coming from legal sources is a key difference between terrorist organizations and traditional criminal organizations involved in money laundering operations. Another difference is that while the money launderer generates income by obscuring the link between the crime and the generated funds, the terrorist's ultimate aim is not to generate income from the fund-raising mechanisms but to obtain resources to support terrorist operations.

1.3. What is Proliferation of weapons of mass destruction?

Proliferation of weapons of mass destruction (WMD) is defined as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials.

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.

1.4. The Need to Combat Money Laundering, Financing of Terrorism and Proliferation of weapons of mass destruction

The Company has three main concerns:

- Reputational Risk;
- Regulatory Risk; and
- Litigation Risk.

The AML requirements focus on the following areas:

- a) Identification procedures;
- b) Record Keeping;
- c) Internal procedures;
- d) Staff Education, Training and Development;
- e) Internal controls and communication procedures that are appropriate for the purposes of forestalling and preventing money laundering and the financing of terrorism; and
- f) Procedures, controls and evaluation.

Irrelevant of how money is transferred to any of our casinos, there is always a risk that this money would have originated from illegal activities, such as credit/debit card fraud, theft from the player's employer or even narcotics trafficking. Hence, by paying greater attention and increase monitoring of high spenders, the Company will be able to mitigate this risk.

2.APPLICABLE RULES AND LEGISLATION

Incorporated and having its statutory seat in Curacao the Company is bound by the local legislation with regards to Anti-Money Laundering and Countering Financing of Terrorism and Proliferation of Weapons. The local authority in charge with the supervision on AML-CFT matters for the gaming sector is the Curacao Gaming Control Board.

The following legislation is applicable to the Company and needs to be taken into consideration within this policy and procedures:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- 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 (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- 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 United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- 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 (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);

- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update May 2024.

The Company checks for amendments to all Decrees and Regulations on a regular basis and updates the policies and procedures accordingly to meet any such changes. Besides these regulatory authorities, the Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ('FATF'), the Caribbean Financial Action Taskforce (CFATF).

3. CUSTOMER ACCEPTANCE POLICY

3.1. Introduction

The Company's general policy is not accepting any players whose funds have emanated from ill-gotten means, and to comply with all applicable obligations in relation to anti-money laundering (AML) and know your customer (KYC). The Company identifies all players prior to establishing a business relationship and proceeds to verify the data provided on certain activities being carried out, which may be first deposit, cumulative deposit thresholds being reached, cumulative withdraw transactions exceeding Naf. 4000 or reaching other triggers. Players who are not registered will not be permitted to play for real money. One of the main drivers is to protect our operations from fraudulent transactions.

It is important that the Company has a clear and concise understanding of all customer practices in order to avoid any possibility of money laundering and/or terrorist financing exposure.

To this end, the Company restricts or prohibits the commencement of business relationships with customers and/or entering into transactions that fall outside our established risk appetite. Therefore, certain categories of individuals are prohibited from being accepted as customers, either by preventing them from registering or by blocking their access to our site, as necessary:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by UN, EU or OFAC.
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity.
- Self-excluded customers who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.
- Individuals who have submitted documents or information that the Company has reasonable grounds to suspect are fraudulent or falsified.
- Customers for whom an elevated risk level in their profile has led the Company to terminate the customer relationship for any reason.

3.2. Age verification

The Company will not accept any player under the age of 18 years (or other age specifically prescribed by law in certain targeted jurisdictions).

3.3. Countries and territories excluded for registration

Below is the general list of banned countries; however, it is not exhaustive and might also include other countries that may have been banned due to various reasons, e.g., change in FATF recommendations, countries banned by license agreements, countries with other deficiencies etc.

1. Afghanistan
2. American Samoa
3. Aruba
4. Australia
5. Belize
6. Belgium
7. Bonaire
8. Bosnia and Herzegovina
9. Burma/Myanmar
10. Burundi
11. Central African Republic
12. Curaçao
13. Denmark
14. Democratic Republic of the Congo
15. Egypt
16. Eritrea
17. Estonia
18. France
19. French Guyana
20. Greenland
21. Guadeloupe
22. Guam
23. Holy See (Vatican City)
24. Italy
25. Iran (human rights)
26. Iran (nuclear proliferation)
27. Iraq
28. ISIL and Al-Qaida
29. Ivory Coast
30. Lebanon
31. Libya
32. Lithuania
33. Kuwait
34. Malaysia
35. Marshall Islands
36. Martinique (.FR)
37. Maldives
38. Mali
39. Netherlands

40. North Korea (Democratic People's Republic of Korea)
41. Occupied Palestinian Territory
42. Poland
43. Puerto Rico
44. Qatar
45. Reunion
46. Republic of Guinea
47. Republic of Guinea-Bissau
48. Saba
49. Saint Barthelemy
50. Saint Martin
51. Saint Pierre and Miquelon
52. Singapore
53. Spain
54. South Africa
55. Somalia
56. South Sudan
57. St. Eustatius
58. Sudan
59. Syria
60. Tunisia
61. USA
62. US Minor Outlying Islands
63. US Virgin Islands
64. Venezuela
65. Yemen
66. Zimbabwe

Also, the Company takes into account a variety of sources concerning geographical risks produced by well-known bodies, including:

- Countries on the FATF list of High-Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement,
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;

- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The Company has its own lists of high, medium and low risk countries that is formed on the basis of recommendations given by the sources listed above, which can be found in [Appendix 1](#).

The Company does not cooperate with- nor onboard clients (players) whose jurisdiction is included in the FATF black list and other sanctions lists, or jurisdictions where the Company has no (appropriate) license to operate.

The following categories of players will not be accepted at registration/post registration checks:

- Players residing in non-reputable or banned jurisdictions,
- IP login registered in a non-reputable or banned jurisdiction,
- Sanctioned individuals, Players under the age of 18.

However, on a case-by-case basis, the Company has the right to refuse any applicant for business or terminate an existing business relationship if the required Customer Due Diligence requirements are not satisfied. A departure from the above, may be applicable, on a case-by-case basis, following the approval of Senior Management.

3.4. Accepted payment methods

The Company accepts payment methods including prepaid cards, mobile payments, internet-based payment services, credit cards, e-wallets, and bank transfers, but does not accept cash. Certain payment methods, such as cash, prepaid cards, and virtual currencies, are considered high-risk as they may disrupt the audit trail and allow customers to maintain anonymity. The Company will only utilize payment methods from licensed financial institutions regulated by an EEA financial regulator.

For internet-based and mobile payment services, the lack of face-to-face contact increases the risk of identity fraud and inaccurate information that could disguise illegal activities. This risk can be mitigated through alternative identification mechanisms, such as credit score checks.

The Company tracks all transactions and ensures that the payouts are returned to the original payment method. If this is not possible, funds will be transferred to an EEA bank account in the customer's name, following the completion of the due diligence process.

Regarding electronic wallets (e-wallets), those that accept funds solely from accounts held in the user's name (e.g., Skrill) do not present a higher money laundering risk than direct funds from financial institutions. However, e-wallets that accept deposits via

prepaid vouchers (e.g., Neteller) carry a greater risk as they can be used to disguise the origin of funds. The Company carefully selects e-wallets, ensuring they are licensed in reputable countries. Due diligence measures, including Know Your Business (KYB) practices and Ultimate Beneficial Owner (UBO) identification checks, are undertaken to identify reputable providers and prevent financial malintent.

The Company identifies specific high-risk payment methods, including cash; anonymous payment methods like prepaid cards and virtual assets; cards issued in the name of third parties; fund transfers between gaming accounts; and financial services such as credit markers, currency exchanges, and check cashing. Some e-wallets may only record payments without detailing the transactions to online casinos, which can enable dishonest customers to disguise their gambling activities.

3.5. No cash policy

The Company does not accept cash deposits nor will cash withdrawals be processed.

3.6. Targeted Financial Sanctions

We are committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with these sanctions. This includes, but is not limited to, the following:

- The Company shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay.
- The Company shall perform perpetual sanctions screening on customers and also perform trigger-based sanctions screening of customers at least in the following scenarios:
 - At the moment of registration;
 - At the moment of withdrawal request;
 - At the moment of any request for change of personal details or payment methods.

In the event that a true match is discovered, the Company shall immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and shall immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, the Company shall terminate services and keep the frozen assets until further instruction from the supervisory authority.

3.7. Politically Exposed Persons (PEPs)

A PEP is 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 the 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 above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, 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.

To identify if a client should be regarded as PEP the Company uses a variety of methods containing sufficient resources. The Company, on an ongoing basis, verifies whether its customers may be considered as PEPs by utilizing open sources and public databases. Should a player who had not been identified as a PEP at on-boarding stage result to have become one, the casino is required to implement the measures described below in 3.7.1 and 3.7.2 within 30 days or terminate the relationship.

The requirements for the CDD of PEPs, as listed below in 3.7.1 and 3.7.2, shall apply also to relatives and close associates of PEPs, as defined in this Policy.

3.7.1. Foreign PEPs

With respect to customers that have been confirmed as foreign PEPs, the Company shall:

- a. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- b. obtain senior management approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction). Senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be given from the manager of the Compliance department;
- c. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the player's spending pattern matches his legal source of funds. The casino requests a statement

from the player about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the information received, the casino can request the customer to provide documents. For PEPs, assessing the source of wealth helps ensure that their overall wealth is consistent with their known income and legitimate activities, thereby mitigating the risk of money laundering or terrorism financing.; and

- d. conduct enhanced ongoing monitoring of the business relationship.

3.7.2.Domestic PEPs

The Company shall take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. In cases of a higher risk business relationship with such persons, casinos are required to apply the measures referred to in items b, c and d section 3.5.1. In accordance with the risk-based approach that the Company employs, measures are tailored to the risk of the PEP, where the following are taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

4. BUSINESS AND CUSTOMER RISK ASSESMENT

4.1. Business Risk Assessment

A BRA is a process whereby the Company identifies the threats and vulnerabilities that it is exposed to and assesses the likelihood and impact of ML/FT risks. On the basis of this assessment, it will be able to determine which areas to prioritize in terms of AML/CFT and ensure that its AML/CFT measures, policies, controls, and procedures are commensurate with the ML/FT risks it faces to mitigate the same. The BRA is therefore the foundation of the risk-based approach and through it the Company can identify and assess the risks of money laundering and funding of terrorism that arise out of its activities or business.

The BRA is based on 4 risk factors:

(a) Customer Risk:

- the number of customers within each customer risk type (e.g. high spenders, disproportionate spenders, PEP);
- the volume of business.

(b) Geographical Risk:

- the number of customers from a given jurisdiction (considering FATF monitored jurisdictions, Global Sanctions listings, countries with high level of corruption, low transparency etc.);
- the number of transactions to/from a given jurisdiction or the customer's connection with any of the jurisdictions as mentioned above.

(c) Products, Services, and Transaction Risk:

- the number and the type of products and services;
- the number of customers per product and service;
- the volume per product and service.
- The number of payment methods used by the customers.

(d) Delivery Channel:

- the number of relationships started on a non-face-to-face basis;

The combination and assessment of these risk factors will allow the Company to identify the threats it is exposed to and the vulnerabilities that may be exploited for ML/FT purposes. Having done so, the Company has to determine the likelihood of any one scenario materializing, and the possible impact thereof. Taken together, likelihood and impact will lead to one's inherent risk.

Likelihood + Impact = Inherent Risk.

Having determined the inherent risk, the Company has to consider what AML/CFT measures, policies, controls, and procedures it already has in place or it plans to adopt

and establish how effective these are in mitigating the inherent risk (Effectiveness of mitigation measures).

At the end the Company can calculate the residual risk:

Level of Inherent Risk – Mitigating Measures = Level of Residual Risk

Even though the Company set out the mitigation measures, there will remain a degree of ML/FT risk that cannot be addressed, avoided, or controlled.

At this stage, the Company has to consider whether the residual risk falls within its risk appetite or to cease the business relationship. The BRA is regularly reviewed on an annual basis. However, the Company revises and updates the BRA:

- (a) whenever new threats and vulnerabilities are identified;
- (b) whenever there are changes to its business model/structures/activities;
- (c) whenever there are changes to the external environment within which the Company is operating.

4.2. Customer risk assessment

The Company understands that its clients will expose it to different levels of risk depending on the particulars of each client, hence it has established a Framework called Customer Risk Assessment (CRA) to identify such risks per client.

The Company has set up the risk factors applicable to all its current participants (new and existing) in order to identify whose circumstances would indicate higher risk and flag them for enhanced due diligence, including enhanced ongoing monitoring, or refusal/termination.

On the basis of the CRA, the Company will be able to apply the proper level of CDD and will be able to identify a customer as presenting a higher risk of ML/FT.

In order to carry out the CRA, the Company should consider all risk factors referred to in this Policy and other risk factors such as:

- a) The Reputation of the customer: the Company should consider whether a customer has been the subject of adverse reports linking him/her to crime (especially financial crimes) and/or terrorism.
- b) Nature and Behavior:
 - the customer is reluctant to provide any documentation and/or information requested by the Company without a legitimate reason for doing so;
 - the documentation presented to meet the Company's request for information/ documentation gives rise to doubts as to its veracity or authenticity.

5. Customer Due Diligence

The Company has an obligation to undertake CDD measures when:

- players engage in financial transactions equal to or above Naf. 4,000.00;
- carrying out occasional transactions above the monetary equivalent of Naf. 4,000.00;
- there is a suspicion of money laundering or terrorist financing; or
- the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows:

- *Identifying* the player and *verifying* that customer's identity using reliable, independent source documents, data or information;
- *Identifying the beneficial owner* and taking reasonable measures to *verify the identity of the beneficial owner*, such that the casino is satisfied that it knows who the beneficial owner is. For legal persons and legal arrangements this should include understanding the ownership and control structure of the customer;
- Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- Conducting *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 casino's knowledge of the player, its business and risk profile, including, where necessary, the source of funds.

The Company's CDD procedures require prospective customers to create a full profile at the point of registration. Mandatory information required at registration stage includes:

- Full name;
- Date of birth;
- Permanent residential address;
- Unique and verified email address;
- Phone number;
- Unique nickname; and
- Password.

To complete the required customer identification and verification process, the Company asks its customers to upload a copy of valid identification documents. This request is sent to the customer's registered email address. If the documents are in a different language, the Company will take necessary steps to ensure that the documents adequately prove the customer's identity, such as obtaining a translation of the relevant parts. This may involve asking the customer to submit documents with a certified true translation.

Only documents issued by government agencies that include a photograph are deemed reliable for verifying the customer's identity. Documents issued by the government that

lack a photograph can be used to confirm the customer's current address, provided the address is included in the document.

If a document submitted by a potential customer does not meet the verification standards, the compliance officer or designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance.

Once a non-compliant document is identified, the customer must be informed without delay. If the customer cannot provide compliant documents within 30 days from the moment the Naf. 4,000.00 threshold is reached, the Company shall terminate the relationship with the customer and report the transaction to the FIU.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

At this stage all customers will be screened through the verification tools including the Sanctions- and PEP lists and adverse media. The Company may also monitor social networks. Sanctioned customers cannot be accepted as customers.

5.1. Simplified due diligence (SDD)

In low-risk scenarios, where the risks of ML/TF/PF are lower, simplified due diligence measures may be applicable, balancing the need for compliance with operational efficiency. Such measures include but are not limited to:

- *Not collecting specific information:* If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity.
- Verifying the identity of the customer and the beneficial owner *after* the establishment of the business relationship;
- The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- The extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- Reducing the frequency of customer identification updates;
- Reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply, or when the customer reaches the threshold prescribed above of Naf. 4,000.00.

5.2. Enhanced Due Diligence

Enhanced Due Diligence (EDD) will be implemented for customers identified as higher risk, consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual. Enhanced Due Diligence has to be conducted where the risks of money laundering or terrorist financing are higher. In any case, the following scenarios are subject to EDD:

- Residents of higher risk geographic areas;
- Politically Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

The applied measures must be consistent with the risks identified. They should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of EDD measures include but are not limited to:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player:
 - **Source of Funds** refers to the origin of the specific funds involved in a particular transaction. This includes identifying how and where the money was generated, such as through salary, business income, or sale of assets.
 - **Source of Wealth**, on the other hand, pertains to the total accumulation of an individual's wealth over time. This includes understanding the broader context of their financial background, such as investments, property ownership, and other significant assets.
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

5.3. Accepted documents

In order to verify the details on their account, the customer is required to send customer care a photocopy or scan of one document from each of the categories listed below:

Personal Identification - one photo ID from the following list:

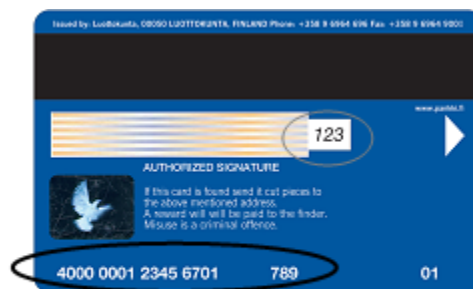
- 1) Current Signed passport
- 2) Current photo-card Driver's License (Provisional or Full)

- 3) Current Full Driver's License (old style paper version)
- 4) Current EU National Identify Card
- 5) Other recognized identity card such as an Armed Forces Identity Card
- 6) Norwegian credit cards with photo and ID numbers can be accepted as ID

Please note regarding some cards from Finland: It can be a debit card and credit card in one, number in the front is for Credit Card and number in the back for Debit Card usually.



Credit-numero etupuolella
Creditillä maksaessasi tarvitset allekirjoituspaneelin vieressä olevan kolminumeroisen tarkistelukuvun.



Debit-numero kääntöpuolella

Address Verification - one of the following:

- 1) Utility bill (within last 3 months)
- 2) Current photo-card Driver's License (Provisional or Full) (Applies for UK DL's)
- 3) Current Full Driver's License (old style paper version)
- 4) ID card with address + Passport or additional ID
- 5) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 3 months)
- 6) Council tax bill or payment book (within last 3 months)
- 7) Recent mortgage statement (within last 3 months)
- 8) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
- 9) Home Insurance certificate or policy
- 10) Motor Insurance certificate or policy
- 11) Electoral roll
- 12) Credit reference agency
- 13) Mobile bills are not accepted

Source of Payment Verification/Proof of Payment - one of the following:

- 1) Company account registered Credit or Debit card
- 2) Copy of Credit or Debit card account statement of a card registered on with Company account (less than 3 months old)
- 3) Copy of bank statement - must have Company transaction or card number visible on it (less than 3 months old)

When requesting such documentation, the customer must always be informed that:

- The card number must be blanked out leaving only the first 6 and the last 4 digits visible together with the expiry date.
- The documents must be clear and legible.
- The documents should show the residential address.

5.4. Enhanced due diligence

Enhanced due diligence (EDD) checks of the customer may be initiated resulting from hits on Sanctions and PEP-lists, residency in high risk geographical areas and through various financial or behavioral triggers, including but not limited to:

- Withdrawal amount;
- Depositing/withdrawing behaviour and pattern;
- Data mismatching;
- Gameplay behaviour;
- Combination of the above.

Depending on the nature of the reason that triggered EDD additional documents next to the ones mentioned above may be requested. These can include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

In carrying out the CDD measures, customers are allowed to continue using their gaming account while the casino obtains any necessary information from the customer concerned. However, If the Naf. 4000, threshold is reached, the player cannot deposit funds into the account or withdraw funds from the account.

Besides that, if the requested information and documentation is not received within 30 days from the moment the Naf. 4000 threshold was met in order for the casino to complete

CDD, the casino has to terminate the relationship with the player and report the transaction to the Financial Intelligence Unit (FIU).

5.5. Methods of verification

From the very moment of registration, all projects' users are constantly monitored by means of our Antifraud System. The System has been configured for the detection of automated and manual suspicions on customers' accounts, for example, multiple account, 3rd party deposits, usage of same deposit methods by several players, potential minor players etc. It also utilizes user verification and pattern detection via machine-learning algorithms. This system is constantly monitored and improved by the relevant staff in order to keep up with the ever-changing fraud patterns and regulatory requirements.

6. TECHNOLOGICAL DEVELOPMENT RISK ASSESMENT

To prevent the misuse of technological developments for the purposes of money laundering and terrorist financing, the Company has implemented a comprehensive set of controls. These controls are designed to identify and assess risks associated with new products, business practices, delivery mechanisms, and emerging technologies. It helps identify and assess the money laundering or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

Controls to Prevent the Misuse of Technological Developments for Money Laundering and Terrorist Financing include:

➤ **Business Partner Verification and Monitoring:**

Enhanced Know Your Business (KYB) Procedures require verification for all new business partners. The Company uses various methods for partners verification through the open check-resources that also include social media.

➤ **Continuous Monitoring:**

The Company monitor business partners behavior with the help of advanced analytics and machine learning algorithms to detect unusual patterns indicative of ML/TF.

➤ **Secure Platform Development:**

The Company uses enhanced security to develop and implement new technological developments, including software and systems. The Company conducts thorough security assessments and penetration testing on new technologies development.

➤ **Data Security:**

The Company shall implement strict access controls to ensure that only authorized employees have access to secure systems and data. The Company develops secure communication protocols to protect customer data and transaction information.

➤ **Product and Service Controls:**

The Company conduct a detailed risk assessment for ML/TF whenever a new product or service is developed, including digital wallets, cryptocurrencies, and peer-to-peer transactions. Implement additional controls and monitoring for higher-risk products and services.

➤ **Ongoing Product Review:**

The Company shall review and update risk assessments and controls for existing products and services to account for new threats and vulnerabilities on a regular basis.

7.ONGOING MONITORING

Once a business relationship has been established the National Ordinance for Identification when rendering services (NOIS) and the National Ordinance Reporting Unusual Transactions (NORUT) require the Company to carry out ongoing monitoring.

It incorporates two key elements:

6.1. Scrutiny and monitoring of transactions:

The Company shall monitor the transactions throughout the course of that relationship to ensure that they are consistent and in line with the customer behavior and his risk profile.

The transactions are monitored in real time (pre-transaction monitoring) and/or after the event (post-transaction monitoring).

Where participants are flagged with a notification after the account opening, accounts are locked until customer due diligence procedures are in place. Some of the possible notifications that can be triggered are:

- SIPs, Watchlist;
- A client residing or located in a country, the AML/CTF/CPF credentials about which the Company has doubts;
- A client who has been the subject of a disclosure;
- A client flagged on the sanctions list;
- A client depositing gambling/withdrawing big amount;
- A client flagged as a fraudster.

To minimize the risks, all payments and fraud agents are instructed to consider instances where a customer uses a card belonging to a third party (i.e. the card holder's name does not match the customer's registered details). Accounts are blocked, explanation and documents requested from the client.

The following transactions or intended transactions are deemed unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- 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);
- Transactions in the amount of Naf. 5000 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 Naf. 5000 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 player.
- Accepting or releasing a deposit in the amount of Naf. 5000 or more at the request of the player;
- Sale to a player of chips in the amount of Naf. 5000 or more. "Chips" include but is not limited to tokens and credits.
- A cash out in the amount of Naf. 5000 or more;

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. 5000.

- Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

The Company is registered with FIU and has access to goAML reporting portal.

7.1. Update the information and the documents of the clients

The Company requests fresh identification documents when the expiry date of identification documents held on file is reached. This can be done on a risk-sensitive basis or be linked to specific trigger events.

Below is a non-exhaustive list of trigger events initiating a player review.

- High deposits/withdrawals;
- Suspicious gameplay activity;
- Non-wagering of funds;
- Mismatch in data (indicated data and/or digital fingerprint data);
- Potential 3rd party usage;
- Potential minor usage;
- Links to other customers.
- Possible hits on screening of Sanctions and PEP-lists.

If the company cannot fulfill the player due diligence requirements, it must either not establish the business relationship or terminate it. The company must document all efforts to obtain the necessary information and documentation. Consequently, the company may choose to close the account or keep it fully blocked and suspended. If the player provides the required information or documentation after the account has been closed or suspended, the company must assess whether the delay impacts the risk of money laundering or terrorist financing associated with the business relationship.

The company should evaluate if there are any reasons to suspect money laundering, terrorist financing, or fraud. A player's reluctance to provide due diligence information should not automatically be seen as suspicious. The company should consider all

available factors and information to determine if there are grounds for suspicion. If there is a presumption of money laundering, terrorist financing, or fraud, the company should report the unusual transaction to the FIU.

If there is no reason to retain the funds, they should be returned to the player through the same channels used to receive them.

8.RECORD KEEPING PROCEDURES

In order to ensure compliance with the PMLFTR (Prevention of Money Laundering and Funding of Terrorism Regulations), the National Ordinance for Identification when rendering services (NOIS) and the National Ordinance Reporting Unusual Transactions (NORUT), as well as implementing procedures the Company ensures that the following records are maintained:

- Record of CRA which is to include the following:
 - a copy of each CRA carried out by the Company.
- Records of CDD information and documents;
- Record of business relationship with the details of transactions;
- Record of internal reports for the Company;
- Record of any determinations made by the Company and the designated employee, where applicable;
- Record of STRs;
- Record of AML/CTF/CPF training;
- Record of conduct certificates or other documentation obtained in carrying out employee screening; and
- Record of any outsourcing agreements.

In accordance with the local legislation the Company maintains all corporate records for a period of 5 years. The period for maintaining records related to AML/CTF/CPF and KYC documents is 5 years or longer when this extension is considered necessary for the purposes of the prevention of ML/TF. The time period commences from the date on which the business relationship is terminated, or the occasional transaction carried out.

The Company maintains these records in electronic form and in its physical files.

9. REPORTING PROCEDURES AND OBLIGATIONS

9.1. Internal Reporting Procedures

By employing the procedures as described in this policy and the Anti-Fraud and AML/CTF/CPF System (the System) fully investigating any transaction, we can identify suspicious transactions or activities that could be construed as money laundering or terrorist financing.

There is an obligation for all staff members to report suspicions of money laundering or terrorist financing, and all suspicions should be reported immediately to the responsible department by completing the Internal Reporting Form.

These reports must be made by the Company's employees when they have a suspicion in relation to a customer's behavior or when they receive an alert from the System based on any transactions that matches the reporting threshold. In the latter case, before submitting a report to the department responsible, the employee must check whether the alert is simply a false positive.

Internal reports are to be submitted in writing using the standard template together with all relevant information and documentation available to the employee to assist the department responsible in making a determination as to how best to proceed. Please see [Appendix 2](#) for the form.

The report must also include details on the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

Where the report is based on the objective indicators, as outlined by pertinent Curacao legislation, such reports shall be submitted to the FIU within 48 hours of the transaction taking place.

Where the report is based on the subjective indicators, as outlined by pertinent Curacao legislation, such reports shall follow the timeline below:

- Internal Unusual Transaction Report (UTR) must be submitted to the Money Laundering Reporting Officer (MLRO) within 24 hours of the transaction taking place
- MLRO must make a determination as to the reportability of the transactions within 10 working days
- If the MLRO determines that the transaction and/or behavior is indicative of ML/TF, the MLRO must submit the report to the FIU within 48 hours of making that determination.

The Company has appointed a Money Laundering Reporting Officer (MLRO) who is responsible for the reporting of unusual transactions to FIU Curacao, as well as other transactions as per guidelines of the local FIU. In addition, the Company has also enlisted the services of a compliance officer, whose tasks involve but are not limited to:

- manage the Customer Due Diligence;
- review of identification documents and information provided by the players at onboarding;
- consulting relevant watch and sanctions-lists;
- conducting further checks where necessary;
- develop and implement an in-house AML training program;
- managing and ensuring that transaction monitoring on players is conducted;
- analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions; and
- report any unusual transactions or activities to the MLRO.

The Money Laundering Reporting Officer (MLRO) must consider, without delay, every internal report received to determine whether or not the information contained in the report: (a) does give rise to a knowledge or suspicion of ML/TF; or (b) whether additional information is necessary to reach this determination.

The responsibilities of the MLRO include but are not limited to:

- Keep records of internally and externally reported unusual transactions;
- Decide whether sufficient suspicion is required to generate reports on money laundering and adequately disclose it to the relevant authorities;
- Verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing; and
- Remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements;

Both the MLRO and the compliance officer shall maintain direct lines of communication with senior management to ensure accountability and transparency, as necessary and with respect to the relevant field of responsibility. Regular report on the status of the AML program, including identified risks, compliance issues, and corrective actions are

provided to the Board of Directors and the CEO. The compliance officer collaborates with other departments, as needed, to ensure a comprehensive approach to compliance.

9.2. External reporting procedures

After considering the internal report and all the necessary documentation, when MLRO determines that there is:

- (a) knowledge;
- (b) suspicion; or
- (c) reasonable grounds to suspect that:
 - a transaction may be related to ML/TF (regardless of the amount involved); or
 - a person may have been, is or may be connected with ML/TF; or
 - ML/TF has been, is being or may be committed or attempted;
- (a) Transaction amounts surpassing the respective thresholds as indicated by the objective indicators.

The MLRO shall file a UTR to FIU Curaçao and determines if reporting should also be done to other FIU in the country of an Outsourcing Provider.¹

The MLRO will not disclose the name of the employee who made the internal report to the FIU, and in completing this report MLRO must provide as much detail as possible together with the relevant identification and other supporting documentation.

The decision to file or not to file an unusual transaction report will always be at the discretion of the MLRO, and MLRO will not be subject to the direction or approval of other parties within the organization, provided that in reaching the decision on whether to file a report, MLRO may seek assistance from other employees of the Company or external advisors.

9.3. Prohibition of Disclosure

The company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU.

¹Outsourcing involves transferring responsibility for carrying out an activity to a third-party provider (“**Outsourcing Provider**”) for an agreed consideration. Outsourced services are usually provided on the basis of a mutually agreed service level as defined in a formal contract.

It is forbidden to disclose information to the customer nor to third parties.

Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

While external disclosure is prohibited, internal communication within the reporting entity may be permitted as necessary to ensure compliance with AML/CTF obligations.

Any disclosure that could prejudice an ongoing or potential investigation by the FIU is illegal.

10. OUTSOURCING SERVICES

Outsourcing involves transferring responsibility for carrying out an activity to a third-party provider (“**Outsourcing Provider**”) for an agreed consideration. Outsourced services are usually provided on the basis of a mutually agreed service level as defined in a formal contract.

Despite the potential benefits of outsourcing, such as the reduction of costs of the company and access to specialized skills, information security incidents, such as inappropriate access to or disclosure of sensitive information, loss of intellectual property protection, or the inability of the outsourcer to abide by agreed service levels, might occur and would reduce the benefits and jeopardize the security status of the organization.

The Outsourcing Policy is available as a stand-alone document. This document (the “Policy”) specifies procedures and controls in place at Hazarion N.V. (the “Organization”) to address and mitigate the risks associated with outsourcing and, in particular:

- Compliance/Regulatory/Legal risks;
- Country risks;
- Operational risks;
- Reputational risks.

And applies to any outsourcing providers including:

- Hardware and software support and maintenance staff;
- External consultants and contractors;
- IT or business process outsourcing firms;
- Temporary staff.

The policy addresses the following controls found under A.15.1 and A.15.2 of the ISO/IEC 27001 and 27002 standards:

- Identification of risks related to external parties;
- Addressing security when dealing with customers;
- Addressing security in third-party agreements.

11. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

11.1. Appointment of a Money Laundering Compliance Officer

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML/CFT compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

11.2. Duties of the Compliance Officer

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

11.3. Employee screening

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing the Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

The employee due diligence process is informed by the Company's risk assessment and the specific roles within the organization.

Any employee whose position may enable them to facilitate money laundering or terrorism financing must undergo screening. This requirement applies to:

- Prospective employees prior to their hiring for such roles.
- Current employees before they are transferred or promoted to such positions.

To screen both current and potential employees, the Company should:

- Identify the individuals.
- Verify their identity.
- Confirm their employment history, such as through references.
- Determine their suitability for the position and assess whether they pose any risk to the Company.

The Company will consider the knowledge and qualifications required for the responsibilities and authorities associated with each role.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.
- The employee has resided in high-risk countries or regions.

Regular updates and re-evaluations are essential for maintaining an effective compliance program against money laundering, terrorism financing, and proliferation financing. This process includes conducting periodic reviews of all employees, with a particular emphasis on those in high-risk roles, to ensure their risk profiles are accurate and current. Additionally, reviews triggered by significant changes in an employee's job responsibilities, promotions, or external alerts that may influence their risk status are also initiated.

11.4. Training

In delivering AML, CTF and CPF training to the designated categories of employees, the Company will consider the necessary knowledge and qualifications required for their duties, responsibilities, and authorizations. As part of the training framework, the Company will outline the AML, CTF and CPF requirements and provide comprehensive information on the measures and activities that staff are expected to undertake within their roles.

The Company will ensure that documentation of the training provided to staff is maintained, capturing the following information:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;

- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

The Company will regularly update the training programs to reflect any changes in internal and external regulations, as well as developments in the availability of training programs in the market for external training. Furthermore, extraordinary training in AML, CTF and CPF matters will be provided in specific situations, including:

- The introduction of new internal and external regulations related to AML, CTF and CPF that apply to the Company's staff.
- The launch of new products or services that alter the AML, CTF and CPF risk exposure.
- Instances where an employee breaches internal or external AML, CTF and CPF regulations due to a lack of knowledge during the performance of their duties.

11.5. Independent audit function

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors.
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

12. REGULARITY OF POLICY UPDATES

The Company must constantly monitor changes in legislation, FATF requirements and the general procedure for combating money laundering and terrorist financing.

The Company checks amendments of Sanctions Decrees and Regulations that are published on the GCB website <https://www.gamingcontrolcuracao.org/> on a regular basis and update its Policies and procedures accordingly to reflect such amendments.

The Company updates its internal anti-money laundering and anti-terrorist financing documents on an ongoing basis, but no later than three months after the entry into force of amendments to anti-money laundering and anti-terrorist financing legislation and / or identifying events that may to impact on AML-CTF-CPF POLICY.

By: Gouloud Hammoud obo Global Related Services B.V.

Date: September 1, 2024

13. APPENDIX 1

LIST OF HIGH-, MEDIUM-, LOW-RISK JURISDICTIONS

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Belarus
5. Bulgaria
6. Burkina Faso
7. Burma (Myanmar)
8. Cameroon
9. Central African Republic
10. China
11. Côte d'Ivoire
12. Croatia
13. Cuba
14. Democratic People's Republic of Korea.
15. Democratic Republic of the Congo
16. Ethiopia
17. Gibraltar
18. Haiti
19. Iran
20. Iraq
21. Kenya
22. Lebanon
23. Libya
24. Mali
25. Monaco
26. Mozambique
27. Namibia
28. Nicaragua
29. Nigeria
30. Panama
31. Philippines
32. Russia
33. Somalia
34. South Africa
35. South Sudan
36. Syria
37. Tanzania
38. Uganda
39. United Arab Emirates
40. Vanuatu
41. Venezuela
42. Vietnam
43. Yemen

Low-risk countries include:

1. Antigua and Barbuda

2. Aruba, Kingdom of the Netherlands
3. Belize
4. Bermuda
5. Cayman Islands
6. Denmark
7. Dominica
8. Finland
9. Grenada
10. Guyana
11. Montserrat
12. New Zealand
13. Norway
14. Saint Kitts and Nevis
15. Saint Lucia
16. Saint Vincent & the Grenadines
17. Singapore
18. Sint Maarten Kingdom of the Netherlands
19. Suriname
20. Sweden
21. Turks and Caicos Islands

By: Gouloud Hammoud obo Global Related Services B.V.
Date: September 1, 2024

14. APPENDIX 2

Internal Unusual Activity Report		
Date of report:		
Client full name:		
Client ID:		
Risk rating:		
Account status (Active/Suspended/Blocked):		
Account balance:		
Date of account registration:		
Client details: E-mail:		
Client details: Phone number:		
Client details: Brand registration:		
Date of birth:		
Nationality/Country of registration:		
Address:	Signature:	Date:
Due diligence documents held:		

Reason for reporting: explain what activity / transaction gave rise to the report. If necessary, please use the additional information section:		
Date of suspected criminal activity/transaction:	Signature:	Date:
Provide details (e.g. dates and amounts) of any known intended or pending transactions:		
Name (reporting employee):	Signature:	Date:
Action taken by the responsible department:		
Confirmation of receipt of the MLRO:	Signature:	Date:

I confirm that I have received this form from the person(s) named above.		
--	--	--

By: Gouloud Hammoud obo Global Related Services B.V.
Date: September 1, 2024