
Anti-Money Laundering & Combating Funding of Terrorism Policy

GRAVITY UNLEASHED BV

1. Document History

Name	Description
Document Name	Anti-Money Laundering & Countering the Financing of Terrorism Policy
Version	1.0
Compliance Officer	Paloma Gonzalez Mascaraque
Contact	Paloma.g.mascaraque@paradym.io
Distribution Date	01.04.2025
Review Date	01.04.2026
Version	1.1
Distribution Date	30.05.2025
Review Date	01.06.2026

2. Table of Contents

1. Document History	2
2. Table of Contents	3
3. Policy Statement	5
4. Background	6
4.1. Money Laundering	6
4.2. How is money laundered?	6
4.3. Terrorism Financing.	7
4.4. How is Terrorism financed?	7
4.5. Common Factors: Money Laundering and Terrorist Financing	8
5. Company's Approach to Money Laundering and Terrorist Financing.	8
6. Business Risk Assessment	8
6.1 Risk Management Process	8
6.2 Risk Identification.....	9
6.3 Risk Assessment	10
6.4 Controls	11
7. Customer Risk Rating & Risk-Based Approach.....	12
8. Know Your Customer & Customer Due Diligence	12
8.1. Background	12
8.2. Simplified KYC and Low Risk	13
8.3. CDD and Medium Risk.....	13
8.4. EDD and High Risk or High Enhance.....	14
8.5. Source of Funds.....	14
8.6 Source of Wealth	15
8.7. Update to Identification Information	16
8.8. Inability to Carry Out CDD Measures	16
9. PEP and SANCTION Screening.....	16
9.1. Politically Exposed Person (PEP)	17
9.2. Sanctions.....	17
10. Reporting Unusual Transactions	17
10.1. Prohibition of disclosure	18
11. Record Keeping	18

12. Monitoring	20
12.1. Areas of monitoring	20
12.1.1. CDD	20
12.1.2. Transaction Monitoring	20
12.1.3. PEP/Sanctions	20
12.1.4 Ongoing Monitoring.....	21
The following periodicity will be applied based on the customer risk profile.	21
13. Education & Training.....	21
14. Red Flags	21
14.1. ML Red flags	21
14.2. Funding of Terrorism Red Flags	22
ANNEX 1.- Customer Acceptance Policy	23
1. Gravity Unleashed BV Policy	23
2. List of Persons not to be accepted/to be terminated	23
3. Accepted Risk	24
- <i>Unacceptable Products/Services/Practices</i>	24
- <i>Acceptable Counterparties</i>	24
- <i>Sufficient Good Standing and Repute</i>	24
- <i>High-Risk Clients</i>	25
4. Country Risk Rating	25
ANNEX 2.- CDD Process – Player Risk Assessment	26
1. Gravity Unleashed BV Policy	26
2. Player Risk Rating	26
3. Risk Based Approach	28

3. Policy Statement

Gravity Unleashed BV (“the Company, us, we”) must implement and maintain robust and effective anti-money laundering (“AML”) and counter-terrorist financing (“CTF”) systems and controls. Following the creation of Gravity Unleashed BV AML Business Risk Assessment, the business has compiled this Manual to assist in the mitigation of its identified risks.

The Company is committed to ensuring that whoever occupies the position of Compliance Officer (“CO”) treats this manual as a live document requiring periodic review and updates where required. All relevant staff is expected to familiarise themselves with this policy and all staff receives AML/CTF training appropriate to their role.

This manual has the below objectives:

- Ensuring the Company’s compliance with all applicable laws, statutory instruments of regulation, and requirements of the firm’s supervisory body.
- Protecting the Company and all its staff as individuals from the risks associated with breaches of the laws, regulations, and supervisory requirements
- Preserving the good name of the Company against the risks of reputational damage presented by implication in money laundering and terrorist financing activities.
- Making a positive contribution to the fight against crime and terrorism.
- Listing the risk mitigation processes to be applied following the Business Risk Assessment exercise.

To achieve these objectives, it is the policy of the Company that:

- Every member of staff shall meet their obligations as appropriate to their role and position in the Group.
- Neither commercial considerations nor a sense of loyalty to customers shall be permitted to take precedence over the company’s anti-money laundering commitment.
- the Company shall appoint an Compliance Officer and where applicable a designated employee to cover in his or her absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out the duties of their appointments.
- The company shall have anti-money laundering policies and procedures outlining the positive actions to be taken by staff in the course of their work, and the Compliance Officer shall keep these under review to ensure their continuing appropriateness.
- The Compliance Officer will monitor the processes and procedures to ensure that they are being correctly administered and adhered to (internal review).

Primarily, the Company is focused on adhering to, among others, the provisions outlined in the following:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
-  National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- 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);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- 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 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 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 10 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);
- 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 Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

4. Background

4.1. Money Laundering

Money Laundering is the process by which criminally obtained money or other assets (criminal property or the proceeds of crime) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins. In this way, criminals aim to disguise the true criminal nature of the assets to make it harder for police or investigatory authorities to seize these criminal assets. Money laundering occurs every time any transaction takes place, or any relationship is formed that involves any form of property that has come from any crime. The key objectives for money launderers are to:

- Disguise the source of criminal property.
- Conceal / distance ownership of criminal property but keep control of it.
- Avoid detection for the underlying crimes; and
- Benefit from the proceeds of crime securely.

Money laundering is a distinctly different crime from the original underlying activity; however, the Company has chosen to put in place controls that make its services unattractive to criminals of all kinds, irrespective of whether the activity taking place is considered to be money laundering.

4.2. How is money laundered?

Money laundering may take a variety of forms and use several methods using all financial services and products. Traditionally the money laundering process comprises three main stages:

1. Placement – where funds from criminal activity are placed into the financial system. For the Company this would be at the point of customer deposits.
2. Layering – Which usually involves a complex system of transactions designed to hide the source and ownership of the funds, and to confuse authorities. For the Company this could for example relate to customers betting equally on red and black in roulette or creating multiple accounts.
3. Integration – where laundered funds are reintroduced into a legitimate economy, appearing to have come from a legitimate source. For the Company, this would be when customers withdraw funds from their accounts.

4.3. Terrorism Financing.

Terrorism is the use or threat of action designed to influence government, intimidate any section of the public, or advance a political, religious, or ideological cause where the action would involve violence, threats to health and safety, damage to property, or disruption of electronic systems.

Terrorist financing is a general term to describe an activity that provides or facilitates the provision of money or property to be used for terrorist purposes.

Traditionally AML efforts have concentrated on the criminalization of the laundering of the proceeds of different forms of underlying criminal conduct. Terrorist financing is a serious threat to financial businesses or businesses where a high volume of monetary transactions takes place. This threat must be taken as seriously as money laundering.

4.4. How is Terrorism financed?

The mainstream methods to raise funds used by terrorist organizations include:

- Private donations by terrorist supporters/sympathizers
- Abuse and misuse of non-profit organizations and charities
- Criminal activity
- Legitimate commercial activity

Terrorist financing often involves a complex series of transactions; like money laundering, this generally follows three separate phases:

1. Collection: funds are often acquired through seeking donations, carrying out criminal acts, or diverting funds from genuine charities.
2. Transmission: where funds are pooled and transferred to a terrorist or terrorist group.
3. Use: where the funds are used to finance terrorist acts, training, materials, accommodation, propaganda, etc.

However, like a three-stage model of money laundering, this model is simplistic and outdated, so it is important not to get caught up in trying to determine if an activity follows this pattern; instead, focus on whether you have knowledge, suspicion, or reasonable grounds to suspect.

4.5. Common Factors: Money Laundering and Terrorist Financing

Factors in common are:

- Laundered proceeds may eventually fund future or prospective criminal acts.
- The destination of money used to support terrorism has to be disguised in the same way that the source of laundered funds must also be disguised.
- Even where the source of funding for terrorist activity is lawful, terrorists will still attempt to disguise it to preserve the future funding stream; and
- Both require the assistance of the financial sector.

4.6 Definition of financing the proliferation of weapons

Proliferation Financing (PF) 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.

5. Company's Approach to Money Laundering and Terrorist Financing.

The Company takes a zero-tolerance approach to money laundering, terrorist financing, and other such financial crimes, and the procedures are maintained to ensure the following:

- The identities of persons conducting business with the Company are adequately identified and verified, and sufficient information is gathered and recorded to permit the Company to 'know its customer' and predict the expected business pattern.
- Potential new relationships that do not appear to be legitimate or where there is suspicion relating to criminal conduct on the potential customer's part are referred to the Compliance Officer before any relationship is entered.
- Established relationships are regularly monitored to ensure they remain fit for the customer's profile, especially regarding large or abnormal transactions.
- Records are retained to provide an audit trail and adequate evidence to the financial information unit or law enforcement for investigatory purposes.
- All suspicions are reported promptly by the internal procedures and, where applicable, reported to the Financial Intelligence Analysis Unit ("FIU") following the relevant procedures.
- The Company has implemented processes that are routinely monitored and tested for effectiveness to help combat money laundering and terrorist financing.

6. Business Risk Assessment

According to the Curaçao Gaming Authority (CGA), each operator shall take steps that are proportionate to the nature, size, and complexity of its activities, in order to identify, assess, and analyse the risks of money laundering and terrorist financing that arise from its business activities.

6.1 Risk Management Process

The company needs to have a risk methodology that establishes a consistent but effective manner for the identification, assessment, and management of money laundering and terrorism financing risks. The below diagram describes the Company's Risk Process flow in terms of money laundering and terrorism financing risks:



6.2 Risk Identification

The Risk Identification refers to the inventory of the business regarding products, customers, countries, staff, and the third-party delegation of AML and CFT functions. The risks listed below under each respective heading are regarded as high concerning money laundering and terrorism financing risk:

Risks related to customers:

- Politically Exposed Persons (PEPs), Relatives and Close Associates (RCAs), or individuals having otherwise prominent public positions that may equally be exploited for their personal advantage;
- Difficulties in establishing source of wealth and/or source of funds;
- Sanctioned individuals or customers or ultimate beneficial owners from sanctioned countries;
- Non-cooperative customers in terms of disclosing information;
- Customers linked to crime (especially financial crimes) and/or terrorism;
- Customers with different and various sources of income;
- Customers involved in high-risk business;
- Customers who have been the subject of the reports submitted to the FIU should be considered as representing a higher risk of money laundering/terrorism financing;
- Low volume activities or irregular activities on the customer's account;
- Customers requesting withdrawals to the bank account of a third party;
- Winner of a bet is different from the person who has originally placed a bet;
- Customers using different payment methods to deposit to their account and request withdrawal to other accounts;
- The IP-address of the customer is different from the residential address of the customer or credit card issuer;

- Customer who has intentionally specified knowingly false or incorrect data.

Risks related to countries, geographical areas and jurisdictions:

- Countries subject to sanctions, embargoes or similar measures issued by the European Union and United Nations (the list of states sanctioned by the EU is available at: <https://sanctionsmap.eu>, the UN sanctioned states list is available at: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>);
- Countries with strategic deficiencies in their regimes to counter money laundering and terrorist financing placed in FATF jurisdictions under increased monitoring list and call for action list (available at: [http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate)));
- Countries having significant level of corruption or other criminal activity (the data is published at transparency international website and jurisdiction is considered as a high-risk if the Corruption Perceptions Index (CPI) is lower than 39 points);
- Countries known by credible sources to support terrorist activities (data is published by the U.S. Department of State and available at: <https://www.state.gov/state-sponsors-of-terrorism>).

Risks related to products and services:

- Fixed-odds games where hedging is possible (blackjack, baccarat, roulette);
- Sports betting;
- Use of payment services providers outside the EU;
- Use of pre-paid cards or vouchers or other anonymous payment methods;

Interface Risk:

- Business is undertaken solely non-face-to-face. The implementation of technological means to address the risk of in personification or identity fraud would significantly reduce the inherent risk.

Staff:

- Governance in ensuring proper and timely compliance with policies and procedures;
- Continuous and effective anti-money laundering and terrorist financing prevention training.

6.3 Risk Assessment

The risk assessment is the result of the likelihood that the Company enables money laundering and terrorism financing multiplied by the impact if a risk materialises. Likelihood is the occasions per period, is something unlikely or likely to happen. Impact is damage or loss to the Company and relative short-term or long-term effects. Likelihood and impact together constitute inherent risk.

Impact Scale

Rating	Variable	Definition
--------	----------	------------

5	Extreme	- Financial loss €100,000 or more - International long-term negative media coverage - Significant prosecution and fines - Withdrawal, suspension of licence or suspension of activities
4	Major	- Financial loss from €70,000 up to €99,999 - National long-term negative media coverage; significant loss of market share - Compliance Officer and/or MLRO resigning - Issues which are considered as severe, but which can be resolved
3	Moderate	- Financial loss from €30,000 up to €69,999 - National short-term negative media coverage - Shortcoming which is considered as minor or not major by the FIU and/or Tax and Customs Board - Widespread staff morale problems and high turnover
2	Minor	- Financial loss from €10,000 up to €29,999 - Local reputational damage - A weakness which is insignificant to be reported to the regulator and authorities and which can be mended
1	Incidental	- Financial loss up to €9,999 - Local media attention quickly remedied - Not reportable to the regulator

Likelihood Scale

Rating	Variable	Definition
5	Almost Certain (AC)	• 90% or greater chance of occurrence over life of asset or project
4	Likely (L)	• 65%-90% chance of occurrence over life of asset or project
3	Possible (P)	• 35%-65% chance of occurrence over life of asset or project
2	Unlikely (U)	• 10%-35% chance of occurrence over life of asset or project
1	Rare (R)	• 10% or lower chance of occurrence over life of asset or project

The results are plotted in line with the attached score table.

		Impact				
		1	2	3	4	5
Likelihood of Occurrence	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

6.4 Controls

Controls are represented by the Rules of Procedure and other Policies that the Company has in place. The effectiveness of controls must be measured in line with the below assessment system:

- **Strong.** Controls are adequate, appropriate, and effective to provide reasonable assurance that risks are being managed and objectives should be met. Policies and their implementation are in line with the respective regulations.

- **Effective.** Compliance Risk is managed adequately and effectively however it could be improved in certain parts.
- **Mostly effective.** Specific control weaknesses were noted; moderate controls; certain improvements are needed.
- **Ineffective.** Compliance Risk is not managed adequately, substantial improvement necessary, but controls have some effect.
- **Non-existent.** No controls, or controls have no effect.

It is important that the Controls are assessed considering Risk Appetite of the Company and are approved by the Board of Directors. This specifically refers to the Customer Acceptance Policy. High risks require more attention, and the Company should dedicate more resources to ensure that the compliance with policies and procedures is properly completed.

7. Customer Risk Rating & Risk-Based Approach

Assessing money laundering or terrorist financing risk is fundamental to the risk-based approach required within our compliance framework.

Within our compliance framework we have the following three risk levels:

-  LOW
-  MEDIUM
-  HIGH
-  HIGH ENHANCE

Our risk assessment is based on four categories:

- Customer
- Geographical
- Interface / distribution channel
- Product Risk

When customers trigger one of these levels, their account is flagged for review to ensure that we hold the correct level of Identification and Customer Due Diligence for their risk.

Defining the individual risk level for every customer allows us to apply a risk-based approach to our due diligence (“DD”) and monitoring. This ensures that we concentrate our resources on the higher-risk areas of our customer database.

The player Risk Assessment Procedure is explained in [ANNEX 2](#)

8. Know Your Customer & Customer Due Diligence

8.1. Background

Know Your Customer ("KYC") is a globally recognized policy designed to mitigate the many financial dangers a business may face, such as money laundering, identity theft, financial fraud, and financing of terrorism.

The primary objective of KYC is to give businesses such as online gaming operators all the information they require to understand their customers better and manage risk accordingly.

It is a regulatory requirement that we have a set of KYC identification procedures to verify customers and their gaming activity.

The Company has a Customer Due Diligence ("CDD") Policy that describes a set of parameters to identify the AML risk a customer may represent. These risk parameters generate a risk score based on the customer's activity, which in turn relates to a KYC requirement for that customer.

Under the applicable law and regulations, we verify and identify our customers as soon as they execute a series of linked transactions that, though individually below the applicable threshold, would cumulatively meet or exceed the XCG 4,000 thresholds. Transactions are considered linked if, for example, they are carried out by the same player through the same game or in one game session.

8.2. Simplified KYC and Low Risk

We need to implement a minimum identification requirement for customers who fall under the low-risk profile.

The identification process begins when the customer requests the first deposit provided by the XCG 4,000 thresholds have not yet been met. This will require the customer to complete the Verification Tab from their gaming account, including the following parameters:

- Name and Surname
- Residential Address
- Date of Birth.

The customer will have 30 days to complete the profile, which will promote the user account to Level 1. If the customer fails to provide the required information within thirty (30) days, the deposit function will be disabled until the user completes the necessary steps.

8.3. CDD and Medium Risk

Medium-risk customers (Level 2) are those who have reached the XCG 4,000 threshold in a single transaction (deposit and/or withdrawal) of linked transactions during the same game session.

The player will upload the scanned copy of one of the following accepted documents at the time of the account registration:

- Passport
- Driver's License
- National ID Card

Through third party Provider SUMSUB, The Company verifies that the scanned document is authentic and the document is not manipulated in any manner and name and photo matches with the Player provided information during the Registration.

The COMPANY will maintain record of the following information for the next five years and will make this information available CGA upon request:

- Plater name and surname
- Type of Document
- Document unique identifying number
- Issuing Jurisdiction and country
- Expiry date (if available)
- Date of identity verification

In the event that the Customer turns out to be a person under the age of 18 due to the compliance department realizing documentation that has been provided is deceptive and misleading, all gambling transactions in which a minor has participated in must be made void, and any amounts gambled must be returned to the related persons' legal guardians.

The customer is required to upload their ID document. If the customer does not provide the required information within thirty (30) days, the cashier option will be blocked until the customer completes this process.

8.4. EDD and High Risk or High Enhance

Continuing with the risk-based approach, the Company has defined a set of triggers that may change the customer's risk profile. The verification team will enhance due diligence ("EDD") to verify further aspects of the player's identity, behaviour, and ability to maintain their level of spending.

For high-risk customers, the Source of Funds and Source of Wealth information must be checked against independent and reliable documentation. This check can be accompanied by an open-source check undertaken of the wealth. Where the client has jumped from low or medium risk to high risk due to the findings from the ongoing monitoring the Company carries out, we may require further independent documents to verify the information provided by the player.

Mandatory Enhanced Due Diligence

The following present situations where enhanced due diligence is mandatory at law:

- Activities or services determined by the FIU to represent a high risk of ML/TF.
- Residents of High-Risk Geographic Areas: Customers residing in jurisdictions associated with higher levels of corruption or inadequate AML, CTF, and CPF regulations
- Transactions or relationships categorized as high-risk by the Company.
- Dealings with persons established in non-reputable jurisdictions.
- Politically exposed persons, family members, and close associates.
- Anonymity-Favoring Products or Transactions: Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.

- **New Products and Business Practices:** The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- *Additional Customer Information:* Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- *Clarification of Business Relationship Intent:* Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- *Source of Funds and Wealth (SOF/SOW):* Gather detailed information on the source of funds or wealth for the player. Examples include:
 - Personal savings
 - Employment income
 - Pension releases
 - Share sales and dividends
 - Property sales
 - Gambling winnings
 - Inheritances and gifts
 - Compensation from legal rulings

In higher-risk situations, Company Name will periodically request SOF information, even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.

- *Transaction Purpose:* Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- **Senior Management Approval:** Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- *Enhanced Monitoring:* Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- *Account Verification for Initial Payments:* Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

8.5. Source of Funds

A customer's source of funds is the actual funds used when making a deposit transaction.

As part of our commitment to preventing our platform from being involved in accepting or processing proceeds of crime, we have internal processes that require customer withdrawals to be sent to the method, channel, or account used to deposit.

While there are occasionally some legitimate reasons for a customer requesting a withdrawal to the method, channel, or account that was not used to deposit, such activity is high risk. Commonly, people will only have one, two, or perhaps three bank accounts at most. If we find that a customer is using an unreasonably high number of accounts to make deposits and/or withdrawals, we must perform a separate in-depth review of their deposit and withdrawal transactions to identify whether the customer has attempted to withdraw to an account that has not previously been used to deposit.

Should a customer be using or be attempting to use a larger number of accounts or deposit methods, we must seek to further confirm that they are the actual holder of the said account or deposit/withdrawal method.

A bank deposit slip or statement which clearly shows the customer's name and account number would be sufficient evidence of ownership of the source of funds.

If we are unable to confirm ownership of the source of funds or if the customer is unwilling to assist in providing evidence of ownership, you should consider whether a Suspicious Transaction Report should be raised to the Compliance Officer.

8.6 Source of Wealth

A customer's source of wealth refers to the origin of the entire body of wealth (i.e. total assets). Source of wealth describes the economic, business, and/or commercial activities that generated, or significantly contributed to, the customer's overall net worth/entire body of wealth, It is how they make their money or have made their money in the past.

It relates to both past and present wealth and:

- It allows us to ensure that the funds they are using to gamble belong to them. The funds could be a current salary or wealth accrued from investments or inheritance.
- It allows us to understand whether funds entering our system may be related to or the proceeds of crime.

A source of wealth may also be any one or combination of the following, this list is not exhaustive:

- Property sales
- Commercial enterprise
- Investment portfolio
- Inheritance
- Gift from Parents/family members
- Compensation or legal settlement
- Betting activities (including accounts with us or our competitors)

The reality is a customer's actual source of wealth may also turn out to be one of the following:

- Drug dealing/smuggling
- Financial crime/fraud
- Identity theft
- Acting as a proxy (registered and bets on behalf of someone else)
- Other criminal activity

8.7. Update to Identification Information

When the customer adds new identification information or updates his identification information, the verification team will perform a second KYC review. Fresh/updated documents will be requested as necessary and must be received within thirty (30) days.

8.8. Inability to Carry Out CDD Measures

Where the Company has been unable to carry out CDD measures within a thirty (30) day period and there are no grounds of suspicion of ML/TF and no STR submitted, or where an STR was submitted but the transaction has not been suspended by the FIU or operation of law or court order, the account is to be closed, and the remaining balance must be remitted back to the player as part of the account closure. The process is to be undertaken under the oversight of the Compliance Officer, who shall ensure that there is no legal impediment to the remittance of the funds and that the funds are only remitted to the same source and channels from which they were received. Where this is not possible, further instructions are to be obtained from the client. When the Company is remitting funds, it must state in the payment details that the funds are being remitted due to the inability to complete CDD.

9. PEP and SANCTION Screening

By the applicable laws and regulations, we are required to check that all customers are not politically exposed persons (“PEP”), associated PEP, or sanctioned persons. This check is undertaken through a third-party service provider SUMSUB’s database which provides publicly available information such as:

- Sanction, watch, regulatory, and law enforcement lists
- Local and international government records
- Country-specific data sources
- International adverse electronic and physical media searches
- English and foreign language data sources
- Relevant industry sources

9.1. Politically Exposed Person (PEP)

A PEP is defined by the Financial Action Task Force ("FATF") as an individual who is or has been entrusted with a prominent public function. Due to their position and influence, it is recognised that many PEPs are in positions that potentially can be abused to commit ML offences and related predicate offences, including corruption and bribery, as well as conducting activity related to terrorist financing. This has been confirmed by analysis and case studies. The potential risks associated with PEPs justify applying additional AML/CFT preventive measures concerning business relationships with PEPs. To address these risks, FATF Recommendations 12 and 22 require countries to ensure that financial institutions and designated non-financial businesses and professions (DNFBPs) implement measures to prevent the misuse of the financial system and non-financial businesses and professions by PEPs and to detect such potential abuse when it occurs.

The following EDD measures are to be applied to all PEPs:

- i. Obtain Compliance Officer approval to service the PEP (Board approval).
- ii. Establish what is their source of wealth and, where applicable, their source of funds; and
- iii. Conduct enhanced ongoing monitoring of the customer's activity.

PEP and sanctioned persons will be screened once the customer reaches the XCG 4,000 thresholds. This shall be repeated within one-eighty 180 days Rolling Period. When a customer not previously identified as a PEP becomes a PEP, the above measures must be carried out within thirty days (30-day window).

9.2. Sanctions

All customers will be checked against relevant sanctions lists at the point that their identity is verified (and then screened on an ongoing basis).

The selection of the sanctions lists is based in the Kingdom of the Netherlands Sanctions act. This check is conducted through our data provider HooYu which is integrated with our onboarding platform and screens against:

- the US Treasury Department's sanction list issued through its Office of Foreign Assets Control (OFAC),
- UN Security Council Committees list of embargoes and asset freezes,
- EU Consolidated list of persons, groups, and entities subject to EU financial sanctions.
- the HM Treasury Consolidated List of Designated Individuals,

The company will not enter a business relationship with any individual or entity with which it is prohibited from dealing by applicable sanctions. If an investigation shows the client is a true match for a sanctioned person or entity, then that match will be reported to the Compliance Officer, who must then determine if any pending transactions should be frozen (if existing client), whether further restrictions should be applied to prevent future transactions, and if the client should be off-boarded.

10. Reporting Unusual Transactions

The Company has set up several measures to:

- a. recognize unusual transactions
- b. document unusual transactions
- c. report unusual transactions

An unusual transaction is one that is inconsistent with the player's profile. Therefore, the first key to recognizing that a transaction is unusual is to know enough about the customer.

As suggested by the applicable Law, the Company may take as unusual the following transactions:
Objective indicators:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural 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)
- c. Transactions in the amount of XCG 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:
 - i. A cashless transaction in the amount of XCG 5,000 or more
 - ii. Accepting or realizing a deposit in the amount of XCG 5,000 or more at the request of the client;
 - iii. Sale to a customer of chips in the amount of XCG 5,000 or more. "Chips" include but it is not limited to tokens and credits.
 - iv. A cash-out in the amount of XCG 5,000 or more.

Subjective indicators:

- d. 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.

By virtue of article 11 of the NORUT, the Company must report unusual transactions or any intended unusual transaction to the FIU without delay.

When preparing an Unusual Transaction Report, The Company is to refer to the **FIU's through the Go AML Portal**.

10.1. Prohibition of disclosure

The Compliance Officer shall submit all unusual transaction reports to the FIU and 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.

The Company and its Officers can never indicate, suggest, or give the impression that an Unusual Transaction Report has been made since any unjustified action may alert the player.

11. Record Keeping

All documents the Company requests to identify or verify individuals and entities are collected electronically. The platform automatically saves transaction records that are accessible only by authorised staff members, whose access to the records is logged and kept on the system.

AML documents are recorded per the regulation and retained in line with the below.

Situation	Documentation (where and as applicable)	Duration
Business relationships and occasional transactions	- Evidence of the CDD (identification and verification) - World Checks/Sanctions Checks - CRA and revisions	5 years from the end of the business relationship or occasional transaction
Details relating to the business relationship and transactions	- Information on the purpose and intended nature of the business relationship - Note for records - Transactions and supporting evidence/records, account files, business correspondence - Signed applications - World Checks/Sanctions Checks	5 years from when the transaction in question was completed – where records relate to the transaction Or 5 years from when the relationship was terminated- where records relate to the relationship
High-risk situations, large and complex transactions	- Reviewing documentation, notes, and records - Transactions	5 years from when the transaction in question was completed
Disclosures made to the FIU	- Unusual transaction reports and supporting documentation	5 years from the event but may be extended by the FIU
Internal reports received by the CO/made to senior management	- Internal suspicious transaction reports and supporting documentation - Reports and analysis of the Compliance Officer	5 years from the event
Training records	- Training log sheet - Presentations /Handouts - Assessments - Certificates	5 years from the event/training
Reports required by the FIU	- Board reports - Compliance Reports	5 years from the date of the report
Risk-Based Approach efforts records	- BRA - Changes to BRA - Records of any decisions taken - Most recent controls, policies, measures, and procedures*	5 years from adoption *from the cessation of activities.
Employee screening records	- Evidence of the CDD such as to conduct certificates and other documents including diplomas, references	5 years from when the employment relationship comes to an end.

Outsourcing and reliance records	- Agreements - Assessments, monitoring	5 years from termination of the arrangement
----------------------------------	---	--

12. Monitoring

The Group's policy is to monitor areas of the business to test for effectiveness in the procedures utilised to mitigate ML & TF. The following monitoring is undertaken by the customer support, verification, and finance teams.

12.1. Areas of monitoring

12.1.1. CDD

Documents provided by customers are reviewed/monitored to ensure that they are fit for purpose, in line with the risk rating and data protection rules. The frequency of this will depend on the risk level attributed to the account. The verification team will address any discrepancy/request with the customer and send a request to update or provide further information.

12.1.2. Transaction Monitoring

To ensure that customers' transactions are not giving cause for concern, i.e., greater frequency, increased level, general behavior outside of the norm, etc. The key requirements of the Company's monitoring framework are that all relevant staff will ensure they monitor and flag:

1. complex or unusually large transactions.
2. unusual, or unusual pattern, of transactions;
3. transactions that have no apparent economic or legal purpose; and
4. any activity that an employee believes is related to money laundering or terrorist financing

12.1.3. PEP/Sanctions

The process used for PEP/Sanction screening should be monitored to ensure:

- Customers have been or will be screened to ensure they are not PEP or Sanctioned persons.

- False positives have been analysed correctly, and information is recorded to show evaluation and decision.
- Confirmed PEPs to ensure the correct level of EDD has been undertaken and that the screening is repeated regularly.
- Teams are following the correct procedure for recording evaluation and analysis.

12.1.4 Ongoing Monitoring

The following periodicity will be applied based on the customer risk profile.

Client Risk Level Monitoring Frequency	
Low	Randomly
Medium	Randomly
High	Every 3 Months
High Enhanced	Every 2 Weeks

13. Education & Training

The company is committed to ensuring that all relevant staff members receive training to fulfil their roles. All new employees, upon commencement of their employment, shall receive the AML and CFT training program, which will include an overview of the subject matter of this Manual.

The Compliance Officer ensures that:

- All management and staff receive initial and ongoing AML/CFT training (at least annually) by various means, which may include online training, face-to-face training, or other applicable methods as determined by the CO from time to time.
- All management and staff are kept informed of updates, policy, or procedural changes as necessary. In some circumstances, staff may be required, whether directly or via their line managers, to confirm they have read and understood the contents of key documents for audit purposes.

14. Audit

The company will outsource its audit function that is independent and responsible for reviewing the internal guidelines, controls and procedures for complying with its obligations under the applicable regulations.

Even though such a function will be outsourced, ultimate responsibility lies with the company. Such function reviews and regularly assesses whether the company's:

- 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.

In addition, the company's AML/CFT policy is audited on an annual basis to ensure the effectiveness of such internal controls. The independent audit function provides recommendations to the relevant persons based on the observations made by such an audit function and ensures that these actions are implemented. The audit shall also evaluate Company Name'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.

Examination by the CGA

Company Name shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the GCB during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

15. Red Flags

15.1. ML Red flags

The following are 'red flags' that could indicate suspicious activity. These examples do not necessarily represent reportable events, but they do suggest situations that may be indicative of activity that should be followed up and clarified:

- The customer does not cooperate in the carrying of CDD
- The customer attempts to register more than one account with the same licensee.
- Customer deposits considerable amounts during a single session.

- Customer deposit funds well more than what is required to sustain his usual betting patterns.
- The customer makes small wagers even though he has significant amounts deposited, followed by a request to withdraw well more than any winnings.
- The customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer inquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- The customer carries out transactions that seem to be disproportionate to his wealth, known income, or financial situation.
- The customer seeks to transfer funds to the account of another customer, or a bank account held in the name of a third party.
- Customer displays suspicious behaviour in playing games that are considered high risk.
- The customer gives insufficient or suspicious information including:
 - unusual or suspicious identification documents that cannot be readily verified.
 - appears to be acting as an agent for an undisclosed principal but is reluctant to provide information.
 - provides information that is inconsistent with the services or facilities that he is seeking; Transactions structured just below a regulatory threshold.
 - questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

15.2. Funding of Terrorism Red Flags

- Transfers to or from areas where terrorist groups are active or are close or have support without any legitimate or reasonable explanation for such transfer.
- Transfer of funds to the same beneficiary account but with the recipient indicated with different names.
- Using pre-payment methods and e-wallets in areas where terrorist groups are active or are close or have support.
- Donations to voluntary organisations having connections with geographical areas with active terrorism.

Version	Description	Date	Contact
1.0	Policy Implementation	01.04.2025	Paloma.g.mascaraque@paradym.io
1.1	Update	30.05.2025	Paloma.g.mascaraque@paradym.io

ANNEX 1.- Customer Acceptance Policy

Customer Acceptance Policy

1. Gravity Unleashed BV Policy

This policy aims to define the company's Client Acceptance Policy ("CAP") in terms of the Regulatory Framework to prevent the use of the Company's products or services for criminal activity.

The Company shall deny establishing or continuing a business relationship with a customer where this relationship is not in line with the CAP.

The Company shall not provide services to the following clients:

- Clients who fall under the list of persons not accepted by the Company, as defined below.
- Clients previously rejected establishing a business relationship with the Company for reasons that continue to exist.
- Clients who have previously had client relationships with the Company have been terminated for reasons that continue to exist.

Key related policies and documents that should be read in conjunction with the CDD Policy are:

- AML/CFT Policy
- CDD Policy

2. List of Persons not to be accepted/to be terminated

The risks posed by the following persons fall beyond the risk appetite of the Company:

1. Persons¹ convicted of a criminal offence.

¹ The term person shall include both natural and legal persons

2. Persons established or operating in, or citizens or resident in, countries subject to EU and UN sanctions or embargoes.
3. Persons established or operating in, or citizens or resident in countries listed in the FATF Category I² jurisdictions.
4. Shell companies and banks.
5. Persons located or operating or residing in high-risk jurisdictions where gambling is prohibited or illegal.
6. Persons whose source of wealth and funds originate from a country subject to EU and UN sanctions or embargoes.
7. Persons whose source of wealth and funds originates from a jurisdiction listed in the FATF Category I.
8. Persons who fail to provide adequate identification and verification information or disclosure of source of wealth/source of funds.
9. Persons who require to have services/accounts provided in the name of anonymous or fictitious persons.
10. Persons subject to sanctions.

3. Accepted Risk

The Company shall accept persons who are located or reside in or whose source of wealth or funds originates from FATF Category II and III jurisdictions. However, these persons shall be marked as HIGH RISK and subject to enhanced ongoing monitoring

- *Unacceptable Products/Services/Practices*

The Company shall not allow or accept the practice of irrational chip dumping in poker games.

- *Acceptable Counterparties*

The Company shall use payment service providers regulated in the EU or EEA; however, payment Providers regulated in a non-EU or EEA area shall be subject to enhanced due diligence.

The Company shall use payment service providers regulated in the EU or EEA; however, payment Providers regulated in a non-EU or EEA area shall be subject to enhanced due diligence.

- *Sufficient Good Standing and Repute*

The Company shall perform independent checks on customers to ensure they are of sufficient good standing and repute.

² Category 1 includes Iran Democratic People's Republic of Korea (DPRK)

- *High-Risk Clients*

Clients' high-risk status shall be determined using the Risk Rating established in the AML CFT Policy and CDD Policy.

Enhanced due diligence measures in line with this Manual shall be applied to all high-risk clients.

Enhanced due diligence measures shall also be mandatory for the following clients:

- *PEPs and family members and close associates.*

Clients engaged in dealings with non-reputable jurisdictions or identified as High Risk according to Appendix 1 of this document will require the approval of the Compliance Officer prior to onboarding high-risk clients and those subject to mandatory Enhanced Due Diligence (EDD).

4. Country Risk Rating

Non-accepted Countries (IP address Block Upon Registration)	High- Risk Countries
Congo, the Democratic Republic	Angola
Curacao	Afghanistan
Iran, Islamic Republic of	Nigeria
Iraq	Lebanon
Libya	Yemen
Myanmar	Mali / Burkina Faso / Niger (Sahel Region)
North Korea	Democratic Republic of the Congo (DRC)
Pakistan	Russia
Syria	Somalia
USA	Sudan
Netherlands	Burkina Faso
Germany	South Sudan
Spain	
France	

ANNEX 2.- CDD Process – Player Risk Assessment

Risk Assessment Procedure

1. Gravity Unleashed BV Policy

The Company as part of its CDD process and legislative obligations, assesses the level of money laundering (“**ML**”) and Anti-financing of Terrorism (“**AFT**”) risk each player poses. This assessment considers the customer, jurisdictional, source of funds, and transaction risks. Product and delivery risk are factored into the AML Business Risk Assessment, as these factors remain the same for all players (i.e. products offered are sportsbook and casino gambling, delivered on a non-face-to-face basis). The objective of risk-based customer due diligence is to ensure that, as the risks within the business relationship increase, the level of information obtained and verified increases proportionally.

Using a risk-based approach will help:

- To determine the level of due diligence required that would be appropriate with the Player’s identified level of risk.
- To determine the frequency of ongoing monitoring and Player information update
- To ascertain the level of management approval required

2. Player Risk Rating

The Company will use a Player Risk-Scoring methodology for Player Risk Assessment, which takes into consideration the following Risk Factors:

- i. Player Information
- ii. Player Transaction history
- iii. Investigative data on the account

Based on player profile information, each player can be assigned with four risk levels:

- I. High Enhance
- II. High
- III. Medium
- IV. Low

Figure 1 Risk Rating Methodology: Extreme and Automatic High-Risk

High Enhance	- PEP associated to high-risk jurisdictions
Automatic High Risk	- Players associated with a high-risk country or Connections to high-risk countries pose a higher risk as those countries may be affected by terrorism, crime or corruption or have ineffective or weak AML standards, making source of wealth a concern along with the detection the suspicious financial or betting activity that makes the company to suspect high probabilities of AML - Players with 2 or more Severe Alerts from Chainalysis - Player with more than 15 UTR within 3 months rolling period.

Figure 2 Risk Rating Methodology: MEDIUM and LOW

For those Players that do not meet any of the criteria to be identified as High Risk or High Enhance, the risk will be calculated from the following three risk categories using the Player Risk Assessment Scoring Mode:

- Player Characteristics
- Transaction Factors
- Investigative Factors

Each risk factor listed above is composed of multiple sub-risk factors.

Depending on the level of risk associated with each factor, each sub-factor is given a score of '15', '10', or '5' points.

Player Characteristics – Weight 30%	
Risk Factor	Score
Full FATF AML/CFT compliance	0
Adverse Media involving money laundering or financial fraud	5
Player is a High-Risk Country Resident	5
PEP or PEP close relative	10
Player with >= 2 Severe Alert in Chainalysis	5
Transaction Factor – Weight 40%	
Deposit & Withdrawal < \$2,000	0
Deposit or Withdrawal Amount in 1 transaction or linked transactions > \$2,000 up to \$20,000	5
Cumulative deposit Amount in 1 month > \$100,000	15
Cumulative deposit amount in 1 month between \$20,000 up to \$50,000	10
Changes on deposit or withdrawal method > 5 times / monthly	5
Minimal or no gaming activity after deposits > \$10,000	5

Player Investigative Factor – Weight 30%	
>= 2 UTR in (1 week)	5
>= 10 UTR in (1 month)	5
>= 0.3 Points BetBy	5
Multiple deposits (BY 3) > €5,000 in 24h => No Game History & request Withdrawal	10
Bonus Abuse Patter	5

The scores are then totalled and weighed together to compute the overall risk score for a Player:

Figure 3 Risk Rating:

Scoring	Risk Rating
<= 3.5	Low
>3.5 and <=6.00	Medium
>6.00 or Automatic high-Risk Factor (PEP)	High
Enhance Risk factor	Enhance High

(Calculate the total for each risk factor and multiply it by the weight, then sum the weighted points)

3. Risk Based Approach

Conducting a risk assessment of each player and assigning a risk level allows The Company to adopt a risk-based approach and allocate its resources appropriately and following the level of ML/TF risk posed by individual players.

The risk-based approach influences the level of CDD required of each player and the level of ongoing monitoring required.

Figure 4 Due Diligence Matrix

Risk assessment	Low Risk (Level 1)	Medium Risk (Level 2)	Medium Risk	High Risk	High Enhance
Source of Wealth					X
Source of funds				X	X
Proof of address			X	X	X
ID verification (SumSub)		X	X	X	X
PEP and Sanction Screening	X	X	X	X	X
Identification: Name & Surname; residential address & DOB	X	X	X	X	X

*****END OF DOCUMENT*****