
Operational Manual

Gravity Unleashed BV

1. Version Control

Name	Description
Document Name	Operational Manual
Version	1.0
Author	Compliance Department
Authorised By	Board of Directors
Distribution Date	01.05.2026
Review Date	01.05.2027

2. Contents

1.	Version Control	2
2.	Contents	3
3.	Introduction	4
4.	Business Model	4
5.	End-To-End Player Lifecycle	4
6.	Regulatory & Compliance Framework	7
7.	Integration of AML Procedures	8
8.	Risk Scoring & Escalation Framework	9
9.	Governance	9
10.	Third-party Management	10
11.	Incident Management	11
12.	Business Continuity	11
13.	Overall Process and Escalation	13

3. Introduction

This Operational Manual delineates the governance structure, procedures, and internal controls overseeing the activities of Gravity Unleashed BV.

The Company functions under license OGL/2024/1052/0508, issued by the Curaçao Gaming Control Board, authorizing the provision of online games of chance via the domain thrill.com.

The manual is in accordance with:

- The Curaçao regulatory framework (NOOGH and transition to Curaçao Gaming Authority)
- International Anti-Money Laundering standards established by the Financial Action Task Force

4. Business Model

4.1 OPERATING MODEL

B2C Online Gaming Operator

Products:

- RNG Casino
- Live Casino
- Sportbook

Target markets:

- Southeast Asia (SEA)
- Latin America (LATAM)
- Africa

4.2 Platform Architecture

- Gaming Platform: Third-party Integration
- Operational Layer: Retool
- Data Analytics: Looker / Internal Engine
- IDV & Pep and Sactions Screen Tool: Sumsub
- Anti-Fraud and Monitoring Tool: Seon
- KYT Tool: Chainalysis
- HR & Payroll Tool: Deel

5. End-To-End Player Lifecycle

Gravity Unleashed BV implements a structured, controlled player lifecycle framework to ensure compliance with regulatory, AML/CFT, fraud-prevention, and responsible-gambling standards. Each phase of the lifecycle is governed by a combination of automated and manual controls designed to identify, prevent, and mitigate financial crime and operational risks.

1. Registration

Players create an account by providing basic personal information, including name, date of birth, email address, and country of residence.

At this stage:

- Minimum age verification (18+) is enforced
- IP address and geolocation checks are performed
- Acceptance of Terms & Conditions and Privacy Policy is required

Accounts are created in a **restricted state** until initial checks are completed.

2. Initial risk screening (geo, device, sanctions):

Upon registration, the player is subject to an automated screening process, including:

- **Geolocation analysis** (country risk, restricted jurisdictions)
- **Device fingerprinting** (to detect multi-accounting or fraud rings)
- **Sanctions and PEP screening** via integrated KYC providers
- **IP consistency checks** (VPN/proxy detection)

3. Deposit (crypto)

Players may fund their accounts using approved payment methods.

Controls applied:

- Wallet screening using blockchain analytics tools
- Payment method ownership verification (where applicable)
- Monitoring of deposit velocity and patterns
- Enforcement of deposit limits (where applicable under RG framework)

Transactions may be restricted or flagged where risk indicators are detected.

4. Gameplay

Once funded, players may participate in gaming activities.

During gameplay:

- Betting patterns are monitored in real time
- Detection of abnormal or suspicious behavior (e.g., low-risk betting, chip dumping, arbitrage patterns)
- Bonus usage is monitored to prevent abuse

Gameplay data feeds directly into the **risk scoring engine**.

5. Continuous monitoring (real-time risk scoring)

All player activity is subject to continuous monitoring through a **dynamic risk scoring system**, which evaluates:

- KYT (Know Your Transaction) alerts
- Transactional behaviour (deposit/withdrawal mismatch, velocity)
- Behavioural indicators (bonus abuse, gameplay anomalies)
- Device and account linkage signals
- KYC status and inconsistencies

Risk scores are updated in real time and determine:

- Account status
- Withdrawal permissions
- Escalation requirements

6. Withdrawal request

7. KYC / EDD (if triggered)

Depending on risk level, the player may be required to provide:

- Identity verification documents
- Proof of address
- Source of funds
- Source of wealth

Failure to complete KYC/EDD may result in:

- Account restriction
- Suspension of withdrawals
- Account closure

8. Approval/rejection

9. Record retention

All player-related data is securely stored in accordance with regulatory requirements.

This includes:

- KYC documentation

- Transaction records
- Risk scores and alerts
- Internal decisions and escalation logs

Records are retained for a minimum of **five (5) years** and are accessible for:

- Regulatory review
- Internal audit
- Law enforcement requests

6. Regulatory & Compliance Framework

Gravity Unleashed BV maintains a **zero-tolerance approach** to:

- Money laundering
- Terrorist financing
- Fraud and financial crime

The Company is committed to operating in full compliance with all applicable laws, regulatory requirements, and international standards, including those established by the Curaçao Gaming Control Board and the Financial Action Task Force.

6.1 Compliance Principles

The Company's compliance framework is built upon the following core principles:

- **Risk-Based Approach:** Resources and controls are allocated proportionately based on identified risks relating to customers, jurisdictions, products, and transactions.
- **Prevention over Detection:** Systems and controls are designed to prevent illicit activity from entering the platform, rather than solely relying on post-event detection.
- **Ongoing Monitoring:** All customer relationships are continuously monitored to ensure consistency with expected behaviour and risk profile.
- **Accountability and Governance:** Clear roles and responsibilities are assigned to ensure effective oversight, including the appointment of a Compliance Officer and MLRO.
- **Auditability and Transparency:** All decisions, actions, and escalations are documented and traceable for internal audit and regulatory review purposes.

6.2 AML / CFT Framework Implementation

As defined in the AML Policy, the Company:

- Applies a risk-based approach to customer onboarding and monitoring

- Conducts Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) where required
- Performs ongoing transaction monitoring to identify unusual or suspicious activity
- Screens customers against sanctions lists and Politically Exposed Persons (PEP) databases
- Maintains comprehensive record-keeping in line with regulatory requirements
- Reports unusual or suspicious transactions to the Financial Intelligence Unit (FIU) without delay

6.3 Compliance Controls

Compliance controls are embedded into the Company's day-to-day operations through a combination of:

- Automated systems (risk scoring engine, transaction monitoring, KYT tools)
- Manual review processes (compliance and fraud teams)

7. Integration of AML Procedures

The AML Policy is integrated through:

- KYC triggers (NAf 4,000 threshold)
- Risk-based monitoring
- Real-time transaction analysis
- Escalation workflows

7.1 Customer Due Diligence (CDD)

Tiered Approach:

- Tier 0: Basic onboarding
- Tier 1: ID verification
- Tier 2: Enhanced Due Diligence (EDD)

EDD triggers include:

- High-risk jurisdiction
- Crypto exposure
- Transaction anomalies

7.2 Ongoing Monitoring

Monitoring includes:

- Transaction behaviour
- KYC consistency
- Risk score evolution

Frequency:

- Low: random
- Medium: quarterly
- High: monthly
- High enhanced: bi-weekly

8. Risk Scoring & Escalation Framework

The Company operates a **real-time risk scoring engine** combining:

- Blockchain analytics (KYT)
- Behavioural monitoring
- Transaction analysis
- KYC status

8.1 Risk Score Inputs

Risk score is derived from:

- KYT alerts (direct/indirect exposure)
- Behavioural triggers (bonus abuse, velocity)
- Deposit/withdrawal mismatches
- Multi-account signals
- KYC inconsistencies

9. Governance

Gravity Unleashed BV operates under a structured governance model designed to ensure **accuracy**,

accountability, and regulatory compliance in all automated and manual decision-making processes.

9.1 Group Governance Principles

Gravity Unleashed BV adheres to group-wide governance principles, including:

- **Centralised Oversight with Local Accountability:**
Strategic compliance oversight is maintained at the group level, while operational execution remains the responsibility of Gravity Unleashed BV.
- **Consistency of Controls:**
Core compliance controls—including AML, fraud prevention, and risk scoring methodologies—are standardised across the group to ensure uniform application of risk management practices.
- **Segregation of Duties:**
Responsibilities are clearly divided across operational, risk, and compliance functions to prevent conflicts of interest and ensure independent decision-making.

9.2 Audit and System Control

Group-level standards require that:

- All decisions are time-stamped
- User actions are attributable to specific individuals
- Logs are retained and accessible for audit and regulatory review

Where applicable, group-wide reporting tools (e.g., analytics dashboards) are used to monitor trends, escalations, and operational performance.

9.3 Approval and Escalation Hierarchy

Critical decisions—including account freezes, high-risk withdrawals, and offboarding—are subject to **dual approval controls**, in line with group policy.

The escalation structure typically includes:

- First-level review by operational AML/Fraud analysts
- Second-level approval by Team Lead or Compliance Officer
- Escalation to group compliance or senior management for complex or high-risk cases

This ensures **multi-layered oversight and decision integrity**.

9.4 Group Compliance Oversight

The Compliance Officer of Gravity Unleashed BV functions within an extensive group compliance framework, guaranteeing conformity with group policies and regulatory standards.

10. Third-party Management

Gravity Unleashed BV engages with a range of third-party service providers critical to its operations, including:

- KYC providers (e.g., Sumsb)

- Payment service providers (crypto and fiat)
- Game and platform providers

The Company ensures that all third-party relationships are managed in accordance with regulatory requirements and internal compliance standards.

11. Incident Management

Gravity Unleashed BV maintains procedures to identify, manage, and report incidents, including:

- AML breaches
- Fraud incidents
- Data breaches

11.1 Process

Incidents are managed through a structured process:

- **Detection:**
Incidents are identified through automated monitoring systems, internal controls, or staff reporting.
- **Escalation:**
Relevant incidents are promptly escalated to the appropriate teams (AML, Fraud, IT, or Compliance) based on severity and nature.
- **Resolution:**
Appropriate corrective actions are taken, including account restrictions, remediation measures, and system fixes where required.
- **Reporting:**
Incidents are documented and, where applicable, reported to the relevant authorities in line with regulatory obligations. All actions are recorded for audit and review purposes.

12. Business Continuity

Gravity Unleashed BV maintains a business continuity framework to ensure the resilience and availability of its services.

12.1 Controls:

- **Backup Systems:**
Critical systems and data are regularly backed up to ensure continuity of operations in the event of disruption.
- **Disaster Recovery:**
The Company maintains disaster recovery procedures designed to restore systems and services within defined timeframes following a major incident.

- **Data Redundancy:**

Data is stored across secure and redundant environments to minimise the risk of data loss and ensure integrity and availability.

13. Overall Process and Escalation

There are no exceptions to this Policy. Any exceptions must be assessed on a case-by-case basis and approved only by the Compliance Officer.

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