
Information Security Policy

Gravity Unleashed BV

1. Version Control

Name	Description
Document Name	Information Security Policy
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.	Scope	4
5.	Company Responsibilities	4
6.	Access Control & Authentication	5
7.	Integration of AML Procedures	6
8.	Risk Scoring & Escalation Framework	7
9.	Governance	8
10.	Third-party Management	9
11.	Incident Management	9
12.	Business Continuity	9
13.	Information Security Objectives	10
14.	Overall Process and Escalation	11

3. Introduction

The aim of the Information Security Policy document is to clearly outline management direction, procedural requirements, and technical guidance to ensure the appropriate confidentiality and integrity of Gravity Unleashed BV's data. It is a priority of the company to ensure that the information has an excellent availability level by providing different means of access and alternatives in case of any failures or problems.

This policy aims to:

- Protect customer, player, and financial data
- Ensure compliance with regulatory requirements (e.g., Curaçao Gaming Authority, data protection laws)
- Mitigate cybersecurity risks
- Maintain operational resilience and system availability

4. Scope

This policy applies to:

- All employees, contractors, and third parties
- All systems, applications, infrastructure, and data
- All physical and cloud environments used by Gravity Unleashed BV

5. Company Responsibilities

5.1 Management

Management is responsible for:

- Approving and enforcing this policy
- Allocating resources for information security
- Ensuring compliance with regulatory obligations

5.2 Chief Technology Officer (CTO)

The CTO is responsible for:

- Maintaining and reviewing this policy periodically
- Ensuring implementation of security controls
- Monitoring compliance and reporting risks
- Ensuring staff receive adequate security training

5.3 Employees and Users

All users must:

- Comply with this policy
- Protect credentials and sensitive data
- Report security incidents immediately

6. Access Control & Authentication

Gravity Unleashed BV shall implement robust access control mechanisms to ensure that access to systems, applications, and data is strictly limited to authorized users and aligned with business requirements.

6.1 Logging Process

Only approved users will be able to access and use the Company's equipment or communications system resources. Positive identification for internal networks involves a user ID and fixed password, both of which are unique to an individual user, or an extended user authentication system.

Access to all systems and data shall be granted based on the principles of:

- **Least Privilege** – Users shall only be granted the minimum level of access necessary to perform their job functions
- **Need-to-Know** – Access to sensitive information shall only be provided where there is a legitimate business requirement

Access rights must be formally approved by management or designated system owners and reviewed periodically.

6.2 Password and Authentication Requirements

A strong password must be enforced, including

- Regular password changes where applicable
- Prevention of password reuse

Passwords must be stored in a secure, hashed, and salted format. Gravity Unleashed BV uses 1Password for this specific purpose, which is used by all employees.

Multi-factor Authentication (MFA) shall be implemented for:

- a. Remote access
- b. Privileged or administrative accounts
- c. Access to critical systems and sensitive data

6.3 Session Management

- User sessions must automatically lock after defined period of inactivity
- Re-authentication is required to regain access
- Session timeouts are configured based on system sensitivity

6.4 Privileged Access Management

Administrative and privileged access must be:

- Restricted to authorised personnel only
- Logged and monitored in detail

Use of privileged accounts is minimised and controlled

6.5 Third-party access

Third-party access must be approved and documented, and restricted to specific systems and timeframes.

Third parties must comply with Gravity Unleashed BV security requirements, and access must be monitored and revoked when no longer required.

6.6

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: Proof of Address
- Tier 3: 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. Information Security Objectives

The overall objectives for information security of the Company are the following:

- Ensure compliance with current laws, regulations and guidelines.
- Ensure the confidentiality, integrity and availability of the Company's information assets
- Ensure the disclosure and mitigation of information security risks
- Ensure the continuous improvement of the information security management system
- Establish controls to protect the Company's information and information systems from harm and loss.
- Ensure the company can continue its operations even if major security incidents occur.
- Ensure the protection of personal data (privacy).
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by the Company.

The company's risk management framework provides the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. Risks will be evaluated through assessing threats and identifying vulnerabilities to critical information assets. The risk assessment and risk treatment plan identify how information-related risks are controlled. CTO is responsible for reducing the risk to an acceptable level. Additional risk assessments may be carried out, where necessary, to determine appropriate controls for specific risks.

All employees of the Company and certain external parties identified in the ISMS are expected to comply with this policy and the ISMS that implements it. All staff will receive appropriate training on information security.

14. 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*****