



AML POLICY

GRACE BAY B.V.

Curacao License no:
OGL/2024/1287/0535



Table of Contents

1. Purpose.....	2
2. Scope.....	2
3. Audience.....	2
4. Definitions	2
5. Roles and Responsibilities	3
6. Regulatory Framework.....	3
7. Risk-Based Approach	3
8. Business and Customer Risk Assessments.....	3
9. Customer Due Diligence (CDD).....	4
10. Enhanced and Simplified Due Diligence	4
11. Politically Exposed Persons (PEPs)	4
12. Ongoing Monitoring	4
13. Reporting of Unusual Transactions.....	4
14. Record Keeping.....	4
15. Internal Controls and Governance.....	4
16. Appointment and Role of the Compliance Officer.....	5
17. Employee Training and Awareness.....	5
18. Independent Audit and Testing	5
19. Review and Approval.....	5
20. Contact Information	5
21. Compliance and Consequences	5
22. Related Information	5
23. Policy History.....	6
24. Policy Access	6

1. Purpose

The purpose of this AML/CFT Policy is to define the standards and procedures adopted by Grace Bay B.V.'s to detect, prevent, and report suspicious activities. The Policy supports Grace Bay B.V.'s goal of complying with applicable legal obligations and fostering a culture of ethical and lawful behavior.

2. Scope

This Policy applies to all Grace Bay B.V. employees, departments, and business units that are involved directly or indirectly in handling customer funds, accounts, data, and gaming operations. It also extends to contractors, service providers, and other external parties operating on behalf of Grace Bay B.V. As a B2C online gaming operator, Grace Bay B.V. interacts directly with end users and is responsible for applying effective Know Your Customer (KYC) and AML controls across all customer-facing processes.

3. Audience

This policy applies to all Grace Bay B.V. employees, directors, officers, contractors, and any third parties engaged in the design, deployment, or management of the Company's operations. It is also applicable to vendors and service providers handling customer identity, funds, or personal data.

4. Definitions

Money Laundering: The process of disguising the origin of illegally obtained money to make it appear as though it comes from a legitimate source.

Terrorist Financing: The act of providing, collecting, or using funds with the intention or knowledge that they will be used to support terrorist activities.

Customer Due Diligence (CDD): The procedures and measures applied to verify the identity of customers and assess the risks associated with them.

Enhanced Due Diligence (EDD): Additional scrutiny and verification procedures applied to customers identified as posing a higher risk of money laundering or terrorist financing.

Politically Exposed Person (PEP): An individual who is or has been entrusted with a prominent public function, including their immediate family members and close associates.

Money Laundering Reporting Officer (MLRO): The designated person responsible for overseeing and enforcing the organization's AML/CFT compliance framework.

Know Your Customer (KYC): The process of identifying and verifying the identity of clients, assessing their financial behaviors and risks.

Unusual Transaction Report (UTR): A report submitted to the Financial Intelligence Unit (FIU) when a transaction or behavior appears suspicious or unusual.

Financial Intelligence Unit (FIU): A national agency responsible for receiving, processing, and analyzing suspicious transaction reports.

Financial Action Task Force (FATF): An intergovernmental organization that sets international standards to combat money laundering and terrorist financing.

5. Roles and Responsibilities

The Board of Directors is ultimately responsible for the implementation and oversight of the AML framework. It approves the AML Policy and ensures sufficient resources are allocated.

The MLRO (Money Laundering Reporting Officer) is the designated individual responsible for ensuring effective implementation of the AML program, reviewing alerts, training staff, and liaising with the CGA and FIU Curaçao.

Employees are expected to comply with this policy, complete all training, and report suspicious activity to the MLRO without delay.

A Deputy MLRO shall be appointed to act in the MLRO's absence.

6. Regulatory Framework

Grace Bay B.V. operates under the Curaçao regulatory framework, complying with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the National Ordinance on Identification of Clients (NOIS), and the Sanctions National Ordinance. These obligations are further defined by the CGA AML/CFT Guidelines. In addition, Grace Bay B.V. adopts best practices from the Financial Action Task Force (FATF) recommendations and monitors global standards that apply to online gaming operators. (CGA AML Policy Jan 2025, p. 6)

7. Risk-Based Approach

Grace Bay B.V. applies a risk-based approach to AML compliance. Each player, product, and channel is assessed based on its risk level. High-risk categories, such as high deposit activity, anonymous payment methods, or foreign IP logins, are flagged for Enhanced Due Diligence (EDD). The risk-based approach guides the depth of due diligence, frequency of reviews, and extent of monitoring. (CGA AML Policy Jan 2025, p. 10)

8. Business and Customer Risk Assessments

Grace Bay B.V. must perform an annual Business Risk Assessment (BRA), covering risks related to gaming platforms, payment processors, jurisdictions, customer types, and delivery channels. In addition, Customer Risk Assessments (CRA) are conducted during onboarding and periodically reviewed. These evaluations help tailor AML controls to user behavior, financial activity, and profile triggers. (CGA AML Policy Jan 2025, p. 11)

9. Customer Due Diligence (CDD)

Grace Bay B.V. must perform CDD on all customers before allowing financial transactions. This includes verifying full name, date of birth, residential address, source of funds, and payment details. Identification is cross-checked against official documents. Players are blocked until CDD is completed. CDD is reapplied when triggers such as high value thresholds, suspicious behavior, or negative media arise.

10. Enhanced and Simplified Due Diligence

Enhanced Due Diligence (EDD) applies to customers with high-risk indicators: high volume deposits, use of anonymous wallets, or activity from sanctioned countries. EDD measures include verifying the source of wealth, source of funds, and increased monitoring. Simplified Due Diligence is rarely used and only under clearly documented low-risk cases, as permitted by CGA. (CGA AML Policy Jan 2025, p. 14)

11. Politically Exposed Persons (PEPs)

All customers must be screened for Politically Exposed Person (PEP) status using an automated KYC tool. PEPs include individuals entrusted with public functions, as well as their relatives and close associates. If identified, the account is escalated for senior management review, subject to EDD, and monitored more closely. Relationships with PEPs require written approval. (CGA AML Policy Jan 2025, p. 15)

12. Ongoing Monitoring

Customer behavior must be monitored in real time using automated systems. Grace Bay B.V. reviews transactions, gameplay patterns, login behavior, and payment activity for anomalies. Any deviation from expected behavior, such as sudden large deposits or play-spend discrepancies, triggers a review by the MLRO. Periodic account reviews are risk-tiered. (CGA AML Policy Jan 2025, p. 15)

13. Reporting of Unusual Transactions

All employees are obligated to report suspicious activity to the MLRO. If the MLRO determines that a transaction or behavior is unusual or potentially related to ML/TF, a UTR is filed with FIU Curaçao. Reporting is not contingent on proving a crime—reasonable suspicion is sufficient. (CGA AML Policy Jan 2025, p. 18)

14. Record Keeping

Grace Bay B.V. must retain all CDD data, transaction logs, and communication records for at least 5 years after the end of a business relationship. Records are stored securely, indexed by user ID, and accessible to the MLRO, compliance team, and regulatory auditors. (CGA AML Policy Jan 2025, p. 21)

15. Internal Controls and Governance

Grace Bay B.V. must maintain a set of internal controls to ensure AML compliance: dual-approval for payouts, role-based access, KYC flags, audit logs, and escalation procedures. All

AML controls are reviewed annually and updated in response to regulatory guidance. (CGA AML Policy Jan 2025, p. 19)

16. Appointment and Role of the Compliance Officer

Grace Bay B.V. must appoint a Money Laundering Reporting Officer (MLRO) who is responsible for implementing this policy, reviewing alerts, submitting UTRs, training staff, and acting as liaison with FIU Curaçao and the CGA. The MLRO reports directly to senior management. A Deputy MLRO is also designated to ensure coverage. (CGA AML Policy Jan 2025, p. 17)

17. Employee Training and Awareness

Grace Bay B.V. must provide AML training to all relevant staff on an annual basis. Training includes red flag indicators, escalation paths, and legal responsibilities. New hires receive onboarding sessions, while the MLRO maintains a log of completed training. (CGA AML Policy Jan 2025, p. 20)

18. Independent Audit and Testing

An external audit of the AML program must be performed every two years. The audit evaluates the effectiveness of internal controls, the adequacy of recordkeeping, and the responsiveness to suspicious activity. Findings are shared with senior management and addressed in remediation plans. (CGA AML Policy Jan 2025, p. 19)

19. Review and Approval

This AML policy is reviewed and approved by the Board of Directors annually. Updates may occur earlier in response to legal changes or audit findings. The MLRO coordinates the review and ensures board approval is documented and filed. (CGA AML Policy Jan 2025, p. 22)

20. Contact Information

For questions regarding this policy or to report a suspicious matter, contact the MLRO:

Email: compliance@gracebaybv.com

21. Compliance and Consequences

Non-compliance with this AML Policy may lead to disciplinary action including suspension, termination, and referral to regulatory authorities. All employees must report breaches or suspicious behaviors in line with internal escalation procedures.

22. Related Information

- National Ordinance on Identification of Clients (NOIS)
- National Ordinance on Reporting of Unusual Transactions (NORUT)
- CGA AML Policy (Jan 2025)
- FIU Curaçao Reporting Guidelines

23. Policy History

Version: 1

Effective Date: June 2025

Reviewed: Annually or as required due to legal changes.

24. Policy Access

The most up-to-date version of this AML policy is available internally at the company offices or can be shared upon request to the Compliance Department.