

ANTI-MONEY LAUNDERING POLICY

Breakout Group B.V.

Version: 4.0

Effective Date: September 25, 2025

Next Review Date: May 25, 2026

Contact:

compliance@breakoutgroup.com



1. Introduction

1.1. It is the policy of Breakout Group B.V. ("the Company") to prohibit and actively prevent money laundering and any activity that facilitates money laundering, terrorist financing, or criminal activity. The Company is committed to full compliance with all applicable laws and regulations, including but not limited to:

1.1.1. the National Ordinance Reporting Unusual Transactions (NORUT),

1.1.2. the National Ordinance Identification when Rendering Services (NOIS),

1.1.3. the National Ordinance Obligations to Report Cross-Frontier Money Transportations, as well as the international standards established by the Financial Action Task Force (FATF).

The Company's AML/CTF framework applies equally to all business activities and transactions, including those processed through the Company's authorized payment agent:

1.1.3.1. HQ Breakout Line Ltd., a Cyprus company, registration number 424448, with offices at Vasili Michailidi 9, 3026 Limassol, Cyprus.

1.2. The Company's senior management is fully committed to implementing and maintaining effective internal systems, procedures, and controls designed to prevent financial crime. These will be regularly reviewed and updated to reflect regulatory changes, best practices, and business needs.

The Company recognizes the distinction between Money Laundering (ML) and Terrorist Financing (TF):

1.2.1. ML involves concealing the origins of criminally derived funds to make them appear legitimate.

1.2.2. TF involves the provision or collection of funds intended to finance terrorist acts or organizations, regardless of whether the funds originate from lawful or unlawful sources.

By adopting this policy, the Company reaffirms its zero-tolerance stance toward financial crime and commits to cooperating with regulators, law enforcement authorities, and international bodies in the fight against ML/TF.

2. Purpose

2.1. The purpose of this Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy is to establish a comprehensive framework of internal controls, procedures, and practices that enable Breakout Group B.V. ("the Company") to:

2.1.1. Prevent the use of its products and services for money laundering, terrorist financing, or proliferation financing.

2.1.2. Ensure compliance with Curaçao national AML/CFT legislation, including but not limited to:

2.1.2.1. the National Ordinance Reporting Unusual Transactions (NORUT),

2.1.2.2. the National Ordinance Identification when Rendering Services (NOIS),

2.1.2.3. the National Ordinance Obligations to Report Cross-Frontier Money Transportations.

2.1.2. Adhere to international AML standards issued by the Financial Action Task Force (FATF) and other relevant authorities.

2.1.3. Protect the Company, its stakeholders, and the integrity of the financial system from criminal abuse.

2.1.4. Define clear roles, responsibilities, and escalation procedures for employees, senior management, and the AML Compliance Officer.

2.1.5. Provide a framework for risk-based monitoring, customer due diligence (CDD), enhanced due diligence (EDD), sanctions screening, suspicious activity reporting, and record keeping.

This Policy also ensures that the Company applies a risk-based approach to customer onboarding, monitoring, and transaction review, with specific measures for Politically Exposed Persons (PEPs), high-risk jurisdictions, and other risk categories.

2.1.6. Furthermore, the Policy provides the foundation for:

2.1.6.1. Annual Business Risk Assessments (BRA) and Customer Risk Assessments (CRA).

2.1.6.2. Internal employee training and awareness programs.



2.1.6.3. Ongoing cooperation with regulators, Financial Intelligence Unit (FIU) Curaçao, and international law enforcement authorities.

2.1.6.4. Independent audits and continuous improvement of AML/CTF practices.

3. Audience

3.1. This Policy applies to the following stakeholders of Breakout Group B.V.:

3.1.1. All members of the Board of Directors and senior management, who bear ultimate responsibility for the implementation of this AML/CTF Policy and are individually accountable for non-compliance.

3.1.2. The AML Compliance Officer (also referred to as the Money Laundering Reporting Officer – MLRO), who is responsible for monitoring transactions, conducting due diligence, reporting suspicious activity to the FIU Curaçao, delivering AML training, and ensuring compliance with regulatory requirements.

3.1.3. All employees of the Company, including but not limited to:

3.1.3.1. compliance, risk, finance, and customer support staff,

3.1.3.2. technical, IT, and security staff with access to player data and systems,

3.1.3.3. marketing, business development, and operational staff interacting with players, suppliers, or partners.

3.1.2. Third-party service providers and outsourced entities, including authorized payment agents (such as HQ Breakout Line Ltd., Cyprus), who must comply with the Company's AML standards and Curaçao regulatory requirements.

3.1.3. Suppliers, contractors, and business partners, who undergo mandatory due diligence checks before entering into a business relationship with the Company.

All employees and third parties subject to this Policy must:

3.1.3.1. Undergo vetting procedures prior to employment or engagement.

3.1.3.2. Participate in initial and ongoing AML/CTF training programs.

3.1.3.3. Familiarize themselves with and adhere to the Company's internal procedures for Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Politically Exposed Person (PEP) screening, sanctions screening, transaction monitoring, suspicious activity reporting (SARs), record keeping, and data protection.

3.1.3.4. Understand that failure to comply with this Policy may result in disciplinary action, termination of employment or contract, civil liability, or criminal prosecution under applicable Curaçao laws and international AML/CFT standards.

4. Definitions

4.1. The Company adopts the following definitions from its AML Policy v4.0:

4.1.2. Money Laundering (ML) – Engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. ML generally occurs in three stages:

4.1.2.1. *Placement* – illicit funds enter the financial system.

4.1.2.2. *Layering* – funds are moved to obscure their criminal origin.

4.1.2.3. *Integration* – funds re-enter the economy appearing legitimate.

4.2. Terrorist Financing (TF) – Providing or collecting funds, whether from legitimate or illegitimate sources, with the intention of using them to support terrorist activities. While ML conceals the source of funds, TF seeks to obscure their destination.

4.3. Anti-Money Laundering (AML) – Legal and regulatory controls that require financial institutions and regulated entities to prevent, detect, and report ML activities.

4.4. Customer Due Diligence (CDD) – Measures undertaken to verify the identity of customers and ensure their transactions are consistent with their known risk profiles.

4.5. Enhanced Due Diligence (EDD) – Additional measures required for high-risk customers, including Politically Exposed Persons (PEPs) and clients from high-risk jurisdictions.

- 4.6. Politically Exposed Person (PEP) – An individual who is or has been entrusted with a prominent public function, or an immediate family member or close associate thereof.
- 4.7. Suspicious Activity Report (SAR) – A mandatory report filed when there is knowledge or suspicion that a person is engaged in money laundering, terrorist financing, or related criminal activity.
- 4.8. Business Risk Assessment (BRA) – An annual documented assessment of ML/TF risks relating to the Company's operations, customer base, jurisdictions, and delivery channels.
- 4.9. Customer Risk Assessment (CRA) – Risk assessment conducted during onboarding to determine the individual risk level of each player, including geographical risk, transaction patterns, employment, and source of funds.
- 4.10. Sanctions Screening – The process of verifying whether customers, suppliers, employees, or partners are listed on international sanctions lists such as those issued by the UN, EU, OFAC (US), HM Treasury (UK), DFAT (Australia), and other authorities.
- 4.11. High-Risk Jurisdictions – Countries or territories identified by the FATF, Curaçao authorities, or other relevant bodies as being under increased monitoring (grey list) or subject to a call for action (black list).
- 4.12. Tipping Off – The unlawful act of disclosing to a person under investigation that a SAR has been or may be filed against them.
- 4.13. AML Compliance Officer / Money Laundering Reporting Officer (MLRO) – The individual appointed by senior management to oversee the AML/CTF program and report to the Curaçao FIU.
- 4.14. Unusual Transaction – A transaction that deviates from the expected pattern of behavior, profile, or source of funds of the player, and which may indicate money laundering, terrorist financing, or criminal activity.

5. Policy Implementation

5.1 Business Risk Assessment

5.1.1. The Company maintains a documented Business Risk Assessment (BRA), conducted at least annually, to identify money laundering (ML) and terrorist financing (TF) risks related to its operations, customer base, jurisdictions, and delivery channels. The BRA shall be reviewed and approved by senior management and made available to regulatory authorities upon request.

The Company's risk-based approach involves the following:

- 5.1.1.1. Identifying ML/TF risks inherent in its business model.
- 5.1.1.2. Designing and implementing policies and procedures to manage and mitigate assessed risks.
- 5.1.1.3. Monitoring and improving the effective operation of controls.
- 5.1.1.4. Maintaining proper documentation of risk assessments.

This approach ensures that AML/CTF efforts are focused where they are most needed and effective. Senior management provides full commitment, and employees actively cooperate in risk management.

5.2 Customer Risk Assessment

5.2.1. The Company conducts a Customer Risk Assessment (CRA) during the onboarding process to determine the risk level of each player. This includes:

- 5.2.1.1. Evaluating geographical risk.
- 5.2.1.2. Reviewing transaction patterns.
- 5.2.1.3. Assessing employment and source of funds.
- 5.2.1.4. Identifying potential red flags.

Based on CRA results, customers are classified by risk level. High-risk categories (including PEPs or customers from high-risk jurisdictions) are subject to Enhanced Due Diligence (EDD).

5.3 Customer Acceptance Policy

5.3.1. The Company applies a risk-based Customer Acceptance Policy (CAP) to ensure proper onboarding. Key principles include:



- 5.3.1.1. Verification of identity through official documents (passport, ID, utility bill, bank statement).
- 5.3.1.2. Assessment of the adequacy of player income compared to spending.
- 5.3.1.3. Application of Enhanced Due Diligence for:

- 5.3.1.3.1. PEPs,

- 5.3.1.3.2. customers from FATF grey- or black-listed countries,

- 5.3.1.3.3. customers with unusual or suspicious patterns.

The Company reserves the right to reject or block accounts if sufficient documentation is not provided or if risks are deemed too high.

5.4 Customer Due Diligence (CDD)

5.4.1. The Company applies the following Customer Due Diligence measures:

5.4.1.1. Verification of customer identity at onboarding through:

- 5.4.1.1.1. Passport or ID card,

- 5.4.1.1.2. Proof of address (utility bill),

- 5.4.1.1.3. Bank statement,

- 5.4.1.1.4. Proof of source of funds,

- 5.4.1.1.5. Proof of income,

- 5.4.1.1.6. Proof of payment method ownership.

- 5.4.1.2. Screening of customers against sanctions lists.

- 5.4.1.3. Screening for PEP status at onboarding and periodically during the relationship.

- 5.4.1.4. Ongoing monitoring of customer activity.

- 5.4.1.6. Where Enhanced Due Diligence is required (PEPs, high-risk jurisdictions, unusual transactions), the Company will:

- 5.4.1.6.1. Obtain senior management approval.

- 5.4.1.6.2. Establish the source of wealth and funds.

- 5.4.1.6.3. Conduct enhanced ongoing monitoring.

Funds must always, where possible, be refunded to the original payment method.

The AML Compliance Officer is responsible for ensuring CDD and EDD procedures comply with Curaçao AML/CFT regulations.

5.5 Ongoing Monitoring

5.5.1. The Company maintains ongoing monitoring of customer identity and transactions to detect unusual or suspicious activity. This includes:

- 5.5.1.1. Reviewing player deposits and turnover to ensure activity aligns with expected behavior.

- 5.5.1.2. Monitoring for mismatched deposits, excessive deposits, or unusual transaction patterns.

- 5.5.1.3. Ensuring that gambling services are not used for money transfers.

- 5.5.1.4. Applying continuous sanctions screening (see Section 24.1).

- 5.5.1.5. Retaining detailed audit trails for all transactions for at least five years.

5.6 Reliance on Third Parties for CDD

5.6.1. Where the Company outsources AML-related activities to third parties, including reliance on third parties for CDD, the Company ensures that such parties:

- 5.6.1.1. Are reputable and subject to equivalent AML obligations.

- 5.6.1.2. Comply with the Company's AML standards and Curaçao regulations.

- 5.6.1.3. Are subject to due diligence and ongoing monitoring by the Company.

- 5.6.1.4. Provide CDD documentation and verification results promptly upon request.

All third-party service providers and business partners undergo risk-based due diligence, including verification of legal status, ownership, and compliance history.

5.7 Reporting of Unusual Transactions



5.7.1. The Company ensures timely and accurate reporting of unusual or suspicious transactions to the Financial Intelligence Unit (FIU) Curaçao, in compliance with national law.

Key principles:

5.7.1.1. Employees must escalate suspicions immediately to the AML Compliance Officer (MLRO).

5.7.1.2. Suspicious Activity Reports (SARs) must be submitted discreetly and confidentially.

5.7.1.3. Tipping off is strictly prohibited and may result in disciplinary and legal consequences.

5.7.1.4. The Company may temporarily or permanently block accounts and withhold funds where suspicion exists.

Employees failing to report suspicions may be subject to disciplinary action or criminal prosecution.

5.8 Anti-Money Laundering Compliance Program

5.8.1. The Company's AML Program establishes minimum standards consistent with Curaçao AML/CFT laws and FATF recommendations.

It includes:

5.8.1.1. A comprehensive framework of policies and procedures to detect and prevent ML/TF.

5.8.1.2. Appointment of an AML Compliance Officer (MLRO) with adequate resources and authority.

5.8.1.3. Independent annual audits of the AML Program by external auditors.

5.8.1.4. Mandatory staff training on CDD, EDD, sanctions screening, and suspicious activity reporting.

5.8.1.5. Clear procedures for escalation, account blocking, and reporting.

5.8.1.6. Regular review and update of high-risk jurisdiction lists (quarterly, based on FATF).

5.8.1.7. Continuous sanctions screening (Section 24.1).

5.9. High-Risk Jurisdictions

5.9.1. In line with Section 15 of the Company's AML Policy v3.0, the following jurisdictions are identified as high-risk according to the Financial Action Task Force (FATF) and other relevant authorities:

Jurisdictions under increased monitoring (FATF Grey List):

- Algeria
- Angola
- Bulgaria
- Burkina Faso
- Cameroon
- Côte d'Ivoire
- Croatia
- Democratic Republic of Congo
- Haiti
- Kenya
- Lebanon
- Mali
- Monaco
- Mozambique
- Namibia
- Nigeria
- Philippines
- South Africa
- South Sudan
- Syria
- Tanzania
- Venezuela
- Vietnam
- Yemen



5.9.2. High-risk jurisdictions subject to a call for action (FATF Black List):

- Democratic People's Republic of Korea (DPRK)
- Iran
- Myanmar

5.9.3. The Company acknowledges that FATF lists are updated periodically and commits to:

- Reviewing and updating its internal lists of high-risk jurisdictions on a quarterly basis,
- Always referring to the most recent official FATF updates if discrepancies arise between internal documents and FATF publications,
- Applying Enhanced Due Diligence (EDD) to all clients residing in these jurisdictions,
- Rejecting onboarding if risks are deemed unacceptable.

5.9.4. If these official lists are updated, but the Company has not yet reflected the changes on its website or internal documents, the Company confirms that it shall refer to the most recent official updates for the purposes of compliance, risk assessment, and due diligence.

6. Compliance and Consequences of Non-Compliance

6.1. Compliance

6.1.1. Breakout Group B.V. is fully committed to compliance with all applicable Curaçao AML/CFT legislation, FATF recommendations, and international best practices. Compliance with this Policy is mandatory for all employees, managers, directors, contractors, suppliers, business partners, and outsourced third parties engaged by the Company.

6.1.2. The Company applies a strict "zero tolerance" approach to breaches of AML/CFT obligations. To ensure compliance:

6.1.2.1. All employees must undergo comprehensive AML/CTF training on:

6.1.2.1.1. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD),

6.1.2.1.2. Identification of Politically Exposed Persons (PEPs),

6.1.2.1.3. Sanctions screening procedures,

6.1.2.1.4. Recognition and reporting of suspicious transactions,

6.1.2.1.5. Consequences of non-compliance.

6.1.3. The AML Compliance Officer (MLRO) oversees adherence to the Policy and reports directly to senior management.

6.1.4. An independent annual audit is performed to evaluate the AML Program's effectiveness.

6.1.5. Internal monitoring and risk assessments are carried out regularly to ensure controls remain adequate and effective.

6.2. Consequences of Non-Compliance

6.2.1. Failure to comply with this Policy, Curaçao laws, or international AML/CFT obligations may result in:

6.2.1.1. For Employees:

6.2.1.1.1. Disciplinary action, up to and including termination of employment.

6.2.1.1.2. Criminal prosecution under Curaçao law for:

6.2.1.1.2.1. failing to report suspicious activity,

6.2.1.1.2.2. non-compliance with disclosure obligations,

6.2.1.1.2.3. tipping off a subject of investigation,

6.2.1.1.2.4. falsification, concealment, or destruction of documents relevant to an investigation.

6.2.1.1.3. Civil liability for damages caused to the Company.

6.2.1.2. For Senior Management:

6.2.1.2.1. Personal liability for consenting to or conniving in AML/CFT offenses.

6.2.1.2.2. Liability for neglect leading to breaches of AML/CFT laws.

6.2.1.3. For Third Parties (suppliers, partners, service providers):

6.2.1.3.1. Immediate termination of contracts or agreements.



- 6.2.1.3.2. Blacklisting from future engagements with the Company.
- 6.2.1.3.3. Legal action to recover damages caused by non-compliance.
- 6.2.1.4. For the Company:
 - 6.2.1.4.1. Financial penalties and regulatory sanctions imposed by Curaçao authorities or international regulators.
 - 6.2.1.4.2. Loss of licenses, reputational damage, and loss of business relationships.
 - 6.2.1.4.3. Freezing of accounts or seizure of assets as ordered by authorities.
- 6.2.2. The Company acknowledges that not escalating a suspicion of money laundering or terrorist financing may lead to criminal prosecution and will treat any breach with the highest severity.

7. Related Information

7.1. General

7.1.1. This AML/CTF Policy must be read in conjunction with, and is supported by, the following internal and external documents, laws, and guidelines.

7.2. Internal Company Policies and Documents

7.2.1. Breakout Group B.V. Privacy Policy (governing the protection and processing of personal data, including customer and employee information).

7.2.2. Breakout Group B.V. Terms of Service, which explicitly prohibit cheating, collusion, and any criminal misuse of the Company's services.

7.2.3. Internal Procedures on Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD), including procedures for PEP screening, sanctions screening, and ongoing monitoring.

7.2.4. Internal Procedures on Suspicious Activity Reporting (SARs), escalation protocols, and whistleblowing mechanisms.

7.2.5. Record Keeping Procedures ensuring availability of audit trails to assist in financial investigations (covering monitoring by the nominated officer, AML/CTF tasks, SARs, training records, communications with authorities).

7.2.6. Employee Vetting Procedures requiring identity checks, reference verification, and background verification.

7.2.7. Internal Information Security and Data Protection Policies, including:

7.2.7.1. System access and authentication controls,

7.2.7.2. Password and malware protection policies,

7.2.7.3. Intrusion prevention and encryption policies,

7.2.7.4. Visitor management and secure storage of equipment and confidential data.

7.2.8. Incident Response Plan for suspected AML/CTF violations, including investigation, reporting, and remediation.

7.3. External Legal and Regulatory Frameworks

7.3.1. National Ordinance Reporting Unusual Transactions (NORUT) – Curaçao.

7.3.2. National Ordinance Identification when Rendering Services (NOIS) – Curaçao.

7.3.3. National Ordinance Obligations to Report Cross-Frontier Money Transportations – Curaçao.

7.3.4. Curaçao AML/CFT National Legislation and Regulatory Directives.

7.3.5. Financial Action Task Force (FATF) Recommendations on Anti-Money Laundering and Counter-Terrorist Financing.

7.3.6. International Sanctions Regimes (as incorporated under Section 24.1, including UN, EU, OFAC (US), HM Treasury (UK), DFAT (Australia), and other applicable lists).

7.3.7. International Best Practices on AML/CTF, as applied in the online gambling sector.

7.4. External Supervisory and Enforcement Authorities

7.4.1. Financial Intelligence Unit (FIU) Curaçao, to which Suspicious Activity Reports (SARs) are filed.

7.4.2. Relevant law enforcement authorities in Curaçao and abroad, for cooperation in criminal investigations.



7.4.3. Regulatory authorities in jurisdictions where the Company or its authorized payment agents operate.

8. Contact Information

8.1. For any questions, clarifications, or reporting regarding this AML/CTF Policy, employees, partners, regulators, or other stakeholders may contact the Company's designated compliance office:

8.1.1. Compliance Officer

Breakout Group B.V.

Email: compliance@breakoutgroup.com

8.2. The Compliance Officer is responsible for:

8.2.1. Overseeing the implementation of this AML/CTF Policy.

8.2.2. Monitoring transactions and ensuring proper reporting of unusual or suspicious activity.

8.2.3. Providing AML/CTF training to staff.

8.2.4. Ensuring continuous compliance with Curaçao legislation and FATF recommendations.

8.2.5. Acting as the Company's primary contact for the Financial Intelligence Unit (FIU) Curaçao and other regulatory authorities.

8.3. Questions regarding this Policy may also be directed to senior management, who retain ultimate responsibility for compliance oversight.

9. Policy History

9.1. Version 4.0 – Effective Date: September 25, 2025.

9.2. Next Review Date: May 25, 2026.

10. Policy URL

10.1. This Policy, once approved and adopted, will be published on the Company's website.

Approved by: eMagnus Curacao B.V.
Managing Director
Breakout Group B.V.
25.09.2025

