Gaming Corps

Anti-Money Laundering and Counter-Terrorist Funding Policy

Gaming Corps AB I 556964-2969 I Postbox 2066, 750 02 Uppsala I www.gamingcorps.com I
info@gamingcorps.com

Contents

Change History

Version	Date	Editor
Current version (v. 7)	**Nov 22, 2025 14:36**	**Anna Azwar Izani**
v. 6	Jul 22, 2025 10:16	Anna Azwar Izani
v. 5	Jun 09, 2025 09:31	Anna Azwar Izani
v. 4	Jun 09, 2025 09:21	Anna Azwar Izani
v. 3	Jun 09, 2025 09:20	Anna Azwar Izani
v. 2	May 12, 2025 08:12	Thomas Elliot Jones
v. 1	May 12, 2025 08:09	Thomas Elliot Jones

1. Purpose

This Policy sets out the framework through which Gaming Corps Malta Ltd seeks to detect and prevent money laundering and the financing of terrorism, in compliance with all applicable laws and regulations. It reinforces our commitment to upholding the highest standards of financial integrity and regulatory compliance.

2. Scope

This Policy applies to all employees, directors, contractors, agents, and individuals acting on behalf of Gaming Corps Malta Ltd.

3. Definitions

Beneficial Owner – A natural person who ultimately owns or controls a customer or on whose behalf a transaction is being conducted.

Business Relationship – A commercial relationship that is expected to have an element of duration, formed in connection with the activities of Gaming Corps.

Customer – A corporate business partner with whom Gaming Corps has or intends to establish a Business Relationship.

MLRO (Money Laundering Reporting Officer) – The person with overall responsibility for overseeing AML/CTF compliance, including transaction monitoring, internal reporting, and liaison with competent authorities.

Nominated Officer – The person appointed by Gaming Corps to receive and assess internal reports of suspicious activity and, where appropriate, file reports with the competent authority.

Politically Exposed Person (PEP) – A person who is or has been entrusted with a prominent public function, including their immediate family members or close associates.

Key Person – The individual certified by the Malta Gaming Authority (MGA) and the UK Gambling Commission (UKGC) and responsible for AML/CTF risk management.

4. Abbreviations

- AML – Anti-Money Laundering
- CTF – Counter-Terrorism Financing
- CDD – Customer Due Diligence
- EDD – Enhanced Due Diligence
- FATF – Financial Action Task Force
- SDD – Simplified Due Diligence
- PEP – Politically Exposed Person
- POCA – Proceeds of Crime Act
- MGA – Malta Gaming Authority
- MLRO – Money Laundering Reporting Officer
- NCA – National Crime Agency (UK)
- FIAU – Financial Intelligence Analysis Unit
- UKGC – UK Gambling Commission

5. Policy Statement

Gaming Corps Malta Ltd (hereafter “Gaming Corps”) is committed to a culture of compliance with all AML/CTF laws and regulations in the jurisdictions in which it operates. The company will not tolerate its services being used for criminal purposes and will actively identify, assess, and mitigate risks associated with money laundering and terrorist financing.

Compliance with this Policy is mandatory for all staff and is overseen by the appointed Key Person and Nominated Officer.

Gaming Corps’s Anti-Money Laundering Regulatory Officer (MLRO and Nominated Officer) is Alex Lorimer.”

6. Compliance Governance

Gaming Corps shall establish and maintain an AML/CTF compliance framework in line with applicable Maltese and UK laws, the MGA, UKGC requirements, and international standards including the FATF Recommendations.

A "risk-based approach" shall be adopted to allocate resources effectively and apply proportionate measures based on the nature and risk level of each business relationship.

7. Risk-Based Approach

Gaming Corps applies a risk-based approach to AML/CTF compliance, enabling the company to focus resources on higher-risk areas. This approach includes:

- Risk assessment of Customers based on jurisdiction, service type, and ownership structure
- Categorisation of Customers into risk levels (e.g. low, medium, high)
- Implementation of appropriate CDD, EDD, or SDD based on the risk level
- Ongoing monitoring and reassessment as needed

The company shall regularly review its risk assessment methodologies and document any updates.

8. Customer Due Diligence

Gaming Corps shall perform CDD measures on all Customers before entering a Business Relationship. The extent and type of CDD shall be proportionate to the risk associated with the Customer.

CDD measures shall include:

- Identifying the Customer (legal entity)
- Identifying beneficial owners and controllers
- Verifying identity using reliable, independent documentation
- Understanding the purpose and nature of the Business Relationship

Where higher risks are identified, Enhanced Due Diligence (EDD) will be applied, including measures such as verifying source of funds and obtaining senior management approval.

Where permitted by law, Simplified Due Diligence (SDD) may be applied in low-risk cases.

9. Customer Acceptance

Gaming Corps shall only onboard corporate Customers that meet the company's AML/CTF standards and provide complete CDD documentation. All Customers must undergo a risk assessment before acceptance.

High-risk Customers, including PEPs or entities linked to sanctions, require additional scrutiny and approval from the Key Person and Board of Directors.

10. Financing

Gaming Corps shall ensure that any form of financing connected to its Business Relationships is subject to appropriate AML/CTF controls. The level of scrutiny shall be proportionate to the risk associated with the Customer, counterparty, or transaction.

Financing measures shall include:

- Verifying the legitimacy and origin of funds
- Assessing whether financing aligns with the Customer's known profile and business model
- Ensuring that payments and transfers occur through regulated and traceable financial institutions

Where higher risks are identified, Enhanced Due Diligence (EDD) will apply, which may include:

- Obtaining evidence of source of funds and source of wealth
- Conducting more frequent reviews of financial activity
- Requiring senior management approval before accepting or continuing financing

Where permitted by law, reduced measures may be applied in low-risk situations; however, Gaming Corps will never accept financing where the source of funds cannot be sufficiently verified.

11. Transaction Monitoring

Gaming Corps conducts ongoing monitoring of all financial transactions related to its customers and other counterparties. The purpose of this monitoring is to identify unusual payment patterns or financial behaviors that may indicate money laundering or terrorist financing risks.

Monitoring activities include:

- Reviewing incoming and outgoing payments to ensure they align with contractual terms and the Customer's known business profile
- Assessing whether revenue flows, invoicing patterns, and settlement structures appear reasonable and consistent
- Ensuring that payments originate from and are sent to regulated financial institutions in the Customer's name
- Identifying unusual or unexplained changes in transaction volume or frequency
- Monitoring for complex, unnecessary, or opaque payment structures that may obscure the true source of funds

Where higher-risk indicators are identified, Gaming Corps may:

- Request additional financial information or documentation
- Verify the legitimacy and origin of funds
- Escalate concerns internally to the MLRO
- Delay or suspend transactions pending further review
- Decline or terminate the Business Relationship where risks cannot be mitigated

When partnering with distributors, aggregators, or operators, Gaming Corps assesses whether the counterparties have adequate AML/CTF controls in place as part of its overall risk evaluation.

12. Ongoing Monitoring

Gaming Corps shall conduct ongoing monitoring of its Customers to ensure:

- CDD information remains current and accurate
- Risk classifications are updated as needed
- Unusual or suspicious activity is detected and assessed

Monitoring frequency is based on the Customer's risk rating:

- High risk – at least annually
- Medium/Low risk – at least every three years

13. Suspicious Activity Reporting

Gaming Corps shall report any suspicion of money laundering or terrorist financing to the relevant authority (e.g., FIAU or NCA) via its Nominated Officer.

All employees must escalate concerns to the Nominated Officer without delay. The company prohibits tipping off and will maintain confidentiality throughout the reporting process.

14. Training

Gaming Corps shall ensure that all relevant employees receive AML/CTF training appropriate to their roles. Training will cover:

- Applicable AML/CTF laws and obligations
- Identification of suspicious activity
- Internal reporting procedures
- Record-keeping and data protection requirements

Training is provided at onboarding and refreshed periodically.

Gaming Corps maintains a central record of all AML/CTF training, including:

- Employee name and role
- Training completion date
- Confirmation of completion

Compliance/HR monitors completion status and issues reminders for overdue training. The MLRO has access to records for audits and regulatory reviews.

15. Policy Review

This Policy shall be reviewed at least annually, or earlier if:

- There are significant changes in applicable AML/CTF laws or regulations
- New business operations or products are introduced
- Regulators issue new guidance