AML Policy – Document Template for License Applicants and Holders

30th January 2026

Approving Official(s):
[Senior administrator(s) responsible for approving the policy.]

Responsible Office:
[Office responsible for policy dissemination, updates, and reviews.]

Effective Date:
[Month, day, and year the policy (or revision) takes effect.]

Next Review Date:
[Month, day, and year for the initial or next scheduled review. New policies or major revisions should be reviewed whenever there are operating environment changes (new games, new markets, new payment methods and regulatory changes). In the absence of such changes, a review is necessary once a year.]

Policy Title

1. Policy Statement

[A clear and concise statement of the Company's commitment regarding the policy's subject matter, including its scope and applicability.]

2. Purpose

[Explain the rationale for the policy, including any legal, regulatory, or business requirements it addresses.]

3. Audience

[Identify the stakeholders affected by the policy, such as "All employees," "Subcontractors," or "Third-party suppliers."]

4. Definitions

[Define key terms with specialized meanings relevant to the policy.]

5. Policy Implementation

[Outline how the policy will be carried out, including key responsibilities and any necessary procedures. Use subheadings for clarity. If procedures are documented separately, specify the responsible department for oversight.]

5.1 Business Risk Assessment (BRA)

[Outline business risk assessment carried out to identify the ML/TF risks you are exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment should address the ways in which the casino's products and services, type of customers, delivery channels and geographical factors could be used to launder money, finance terrorism and finance proliferation, and the extent of the risk that this will happen. In this respect the casino should indicate risk it is prepared to accept. Furthermore, it should indicate how effectiveness of the measures to mitigate risks are monitored and improved. Revision of the BRA should happen whenever changes occur to the operating environment, otherwise once a year. The BRA should be documented and approved by management. Technological development risk assessment should be carried out prior to launch of new products, business practices, delivery mechanism or new technologies.]

5.2 Customer Risk Assessment (CRA)

[The Customer Risk Assessment will assess the particular risks the casino will be exposed to when providing its services or products to players. The information collected to draw up the CRA will formulate the customer's risk profile. The customer specific risk assessment has to be carried out during establishing a business relationship. The categories follow from the BRA.]

5.3 Customer Acceptance Policy

[On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy (CAP). When drawing up its CAP the casino has to comply with its obligations with regard to Politically Exposed Persons (PEP) and Sanctions Screening. The CAP should address the type of players that pose higher than average risk and also indicate the circumstances under which a player is denied.]

5.4 Customer Due diligence

[Describe timing and which measures are used for customer due diligence including PEP and sanction screening. Further describe the actions taken when XCG 4,000 is reached, but not all documents have been submitted by the player. Describe what happens if the requested information is still not received within 30 days of reaching the threshold. Describe the process if the business relationship needs to be terminated.

Describe the timing of ongoing sanctions screening (UN and EU list) and the procedure followed for freezing of funds and reporting to competent authorities in Curacao.]

5.5 Ongoing Monitoring

[Describe the measures employed for ongoing monitoring of customers identity and transactions]

5.6 Reliance on third parties to perform customer due diligence

[Describe if the operator relies on third parties for CDD and how that is arranged]

5.7 Reporting of unusual transactions

[Describe the process in place to recognize and report unusual transactions to the Curacao FIU when threshold of XCG 5000 is reached. Please note the prohibition to disclose a report filed to the FIU. The record keeping requirements for CDD information and transactions needs to be described.]

5.8 Anti-Money Laundering Compliance program

[An AML program should be risk-based and should be designed to mitigate the money laundering and terrorist financing risks the organization may encounter. The AML program should establish minimum standards for the organization that are reasonably designed to comply with applicable laws and regulations.]

6. Compliance and Consequences of Non-Compliance

[Describe the risks and potential consequences of violating the policy, including disciplinary actions, legal implications, or business risks.]

7. Related Information

[Provide links or references to related policies, legal or regulatory frameworks, guidelines, or relevant forms and templates.]

8. Contact Information

For any questions regarding this policy, please contact:

[Insert name/office, phone number, and email address.]

9. Policy History

[Indicate whether this is a new policy or if it replaces an existing one. List previous versions with effective dates and revisions, if applicable.]

10. Policy URL (if applicable)

[Indicate where the policy can be accessed online if published on the Company website.]