Anti-Money Laundering (AML) Code of Conduct for Internet Gaming Operators Issued by Anjouan Licensing Services Inc.

Introduction

This **AML Code of Conduct** establishes the responsibilities and requirements for Internet Gaming Operators licensed on the **Autonomous Island of Anjouan** to prevent money laundering (ML) and the financing of terrorism (FT). Operators are required to implement policies, procedures, and controls that comply with local laws, international best practices, and standards such as the **Financial Action Task Force (FATF) Recommendations**.

Scope

This Code applies to:

1. All licensed Internet Gaming Operators.
2. UBOs, shareholders, directors, key personnel, employees, and agents involved in gaming operations.
3. Any third-party service providers contracted by operators.

Failure to adhere to this Code may result in penalties, including fines, license suspension, or revocation.

---

1. Legal and Regulatory Framework

Operators must comply with:

- **AML/CFT Laws of the Autonomous Island of Anjouan**.
- International standards, including FATF Recommendations.
- Any directives issued by **Anjouan Licensing Services Inc**.

---

2. Core Principles

1. **Risk-Based Approach**: Tailor AML/CFT measures to the level of risk identified in operations.
2. **Transparency**: Ensure full traceability of funds and prevent anonymous gaming activities.
3. **Accountability**: Establish clear lines of responsibility within the organization for AML compliance.
4. **Collaboration**: Cooperate fully with regulatory authorities and AOFA.

---

3. Risk Assessment

3.1 **Risk Identification**

Operators must conduct a comprehensive risk assessment to identify ML/FT risks based on:

- Player profiles (e.g., geographic location, financial history).
- Products and services offered.
- Delivery channels (e.g., online platforms, payment methods).
- Jurisdictions involved (e.g., high-risk countries).

3.2 **Risk Mitigation**
Based on the risk assessment, operators must:

- Implement proportionate controls.
- Apply enhanced due diligence (EDD) for high-risk scenarios.
- Review and update the risk assessment annually or upon major operational changes.

---

4. Customer Due Diligence (CDD)
4.1 **Player Identification**
Operators must verify the identity of all players upon first withdrawal request, regardless of amount or when total Cumulative deposits reach US $10,000 or equivalent. Required information includes:

- Full legal name.
- Date of birth.
- Nationality.
- Residential address.
- Government-issued photo identification.

4.2 **Verification**
Verification must be conducted through:

- Certified copies of identification documents.
- Independent electronic verification services.
- Official utility bills or bank statements for address confirmation.

4.3 **Threshold for Verification**
CDD must be conducted when:

- Cumulative deposits reach $10,000 USD or equivalent
- On first withdrawal regardless of amount.
- Suspicious activity is detected, regardless of the transaction amount.

4.4 **Enhanced Due Diligence (EDD)**
EDD is required for:

- Politically exposed persons (PEPs) and their family members or associates.
- Players from high-risk jurisdictions identified by FATF.
- Complex or unusually large transactions with no apparent economic purpose.

---

5. Record Keeping
5.1 **Retention Period**
Operators must retain the following records for at least five (5) years:

- Player identification and verification documents.
- Transaction logs, including deposits, wagers, and withdrawals.
- Suspicious activity reports (SARs).
- Internal audit and compliance reports.

5.2 **Accessibility**
Records must be stored securely and made available to regulatory authorities upon request.

---

6. Monitoring and Reporting

6.1 **Transaction Monitoring**

Operators must implement systems to monitor and analyze player transactions for:

- Unusual patterns (e.g., frequent deposits just below reporting thresholds).
- Rapid movement of funds between accounts.
- Transactions involving high-risk jurisdictions.

6.2 **Suspicious Activity Reporting (SARs)**

- Suspicious transactions must be reported to Anjouan Licensing Services Inc. within 24 hours of detection.
- Include detailed descriptions of the activity, player information, and supporting evidence.

6.3 **Currency Transaction Reports (CTRs)**

- Report all transactions or group of linked transactions exceeding $10,000 USD or equivalent, to Anjouan Licensing Services Inc., even if no suspicion arises.

---

7. Internal Controls

7.1 **AML Policies and Procedures**

Operators must establish written policies and procedures covering:

- Risk assessment and management.
- CDD and EDD processes.
- Monitoring and reporting mechanisms.

7.2 **Compliance Officer**

Each operator must appoint a **Compliance Officer** responsible for:

- Overseeing AML compliance.
- Acting as the point of contact for the FIU and regulatory authorities.
- Ensuring timely submission of reports.

7.3 **Employee Training**

All employees must receive regular AML training, which includes:

- Identifying red flags and suspicious activity.
- Conducting CDD and EDD.
- Filing SARs and CTRs.

Training must be provided:

- Upon hire.
- Annually.
- Whenever there are changes in regulations or company policies.

---

8. Cybersecurity and Data Protection

8.1 **Data Integrity**

Operators must ensure that player data is accurate, complete, and protected against unauthorized access or alteration.

8.2 **System Security**

- Use robust cybersecurity measures, including firewalls, encryption, and intrusion detection systems.
- Conduct regular vulnerability assessments and penetration testing.

8.3 **Breach Reporting**
Any cybersecurity breach or data theft must be reported to Anjouan Licensing Services Inc. within 24 hours.

---

9. Independent Audits
9.1 **Annual AML Audit**
Operators must undergo an independent AML audit annually to evaluate:

- Effectiveness of AML/CFT policies and procedures.
- Compliance with legal and regulatory requirements.
- Adequacy of training and internal controls.

9.2 **Regulatory Oversight**
Anjouan Licensing Services Inc. reserves the right to conduct random inspections and audits of licensed operators.

---

10. Penalties for Non-Compliance
Non-compliance with this Code may result in:

1. Fines or monetary penalties.
2. Suspension or revocation of the gaming license.
3. Referral for criminal prosecution in cases of deliberate violations.

---

11. Continuous Improvement
Operators are encouraged to:

- Stay updated on changes in AML/CFT regulations.
- Adopt emerging technologies, such as AI and blockchain, to enhance monitoring and compliance.
- Participate in industry forums and training programs to align with international best practices.

Acknowledgment
All licensed operators must acknowledge and agree to comply with this AML Code of Conduct as a condition of their licensing. Failure to do so may result in enforcement actions as deemed appropriate by Anjouan Licensing Services Inc.