AML CODE OF PRACTICE FOR REMOTE AUTHORITY LICENSE HOLDERS

Issued by the Sovereignty Authority
Effective Date: 05/05/2025

1. Introduction

This Code of Practice sets forth mandatory Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) obligations for all Remote Authority License Holders ('Licensees') under the Sovereignty Authority...

2. Scope and Applicability

This Code applies to all entities licensed to operate remote gambling, digital assets, gaming, lottery, or financial services within or under the Sovereignty Authority...

3. Governance and Responsibility

- Money Laundering Reporting Officer (MLRO): Licensees must appoint an MLRO...
- Senior Management Accountability: The board must actively oversee AML programs...
- Training Programs: Staff must receive annual AML training...

4. Customer Due Diligence (CDD)

All Licensees must:

- Verify identity using government-issued photo ID...
- Implement KYC procedures...
- Apply Enhanced Due Diligence (EDD)...

5. Risk Assessment and Controls

Conduct a documented Business Risk Assessment (BRA) at least annually...
Implement monitoring systems capable of identifying patterns of suspicious or abnormal behavior.

6. Suspicious Activity Reporting (SAR)

Licensees must submit SARs to the Sovereignty Authority's Financial Intelligence Unit (FIU)...
Reporting must be confidential...

7. Recordkeeping

Licensees must retain the following for at least five (5) years:
- Customer identification documents
- Account records and transaction logs...

8. Technological Safeguards

Use geo-IP filtering, deploy automated transaction monitoring systems, prohibit the use of mixers, tumblers, or privacy coins unless risk-assessed...

9. Virtual Asset Service Providers (VASPs)

VASPs must adhere to the following:
- Comply with the Travel Rule...
- Monitor wallet addresses and DEX interactions...
- Maintain on-chain and off-chain traceability...

10. DeFi and Smart Contract Obligations

Where DeFi operations are concerned, Licensees must:
- Conduct smart contract audits
- Ensure KYC-gated interfaces...
- Prevent use by restricted jurisdictions...

11. Sanctions and Restricted Country List

1. Licensees must block access from the following countries:
   1 Afghanistan
2. Belarus
3. Central African Republic
4. Crimea Region
5. Cuba
6. Democratic People's Republic of Korea (North Korea)
7. Democratic Republic of Congo
8. Eritrea
9. Iran
10. Iraq
11. Lebanon
12. Libya
13. Mali
14. Nicaragua
15. Russia
16. Somalia

17. South Sudan
18. Sudan
19. Syria
20. Venezuela
21. Yemen
22. Zimbabwe

These jurisdictions are subject to international sanctions, FATF “blacklist” designation, or exhibit systemic AML deficiencies.

12. Enforcement and Penalties

Non-compliance may lead to civil and criminal penalties, public revocation of licensing, asset freezing...

13. Amendments and Reviews

This Code is reviewed annually or as deemed necessary by the Sovereignty Authority...