NIISITAPI
GAMING COMMISSION

Combating of Money Laundering, the Financing of Terrorism, and the Financing of Proliferation of Weapons of Mass Destruction

Document control

Item	Entry
Issued by	Niisitapi Gaming Commission
Applies to	All licensees of the Commission offering games of chance, sports and event wagering, and other online games from the Territory
Legal basis	Regulations 13.1(m), 21 and 46 of the Online Gaming Regulations
Version	1.0
Effective date	1st December 2026
Policy owner	Niisitapi Gaming Commission
Review cycle	At least every two years, and after any significant regulatory change (Part I.5)
Enquiries	Refer to the Niisitapi Gaming Commission website

Contents

Document control 1
1. General Statement and Purpose 4
2. Application 4
3. Effect 4
4. Legal Authority and Regulatory Status 5
5. Functions and Powers of the Commission 5
6. Inter-Agency Cooperation 6
7. Obligation of Confidentiality 6
II.1 General Statements 7
II.2 What is Money Laundering? 7
II.3 What is Financing of Terrorism? 7
II.4 What is Financing of Proliferation of Weapons? 8
II.5 Targeted Financial Sanctions 8
III.1 What is the Risk-Based Approach? 10
III.2 The Business and Customer Risk Assessments 10
III.2.1 Business Risk Assessment (BRA) 10
III.2.2 Customer Risk Assessment (CRA) 11
III.2.3 Risk Factors Specific to the Gaming Sector 11
III.3 Technological Developments Risk Assessment 13
IV.1 Introduction 14
Use of Physical Establishments 14
IV.2 The CDD Measures 15
IV.2.1 Identification and Verification of the Player 15
IV.2.2 Identification and Verification of the Beneficial Owner 16
IV.2.3 Purpose and Intended Nature of the Business Relationship 16
IV.2.4 Ongoing Monitoring 17
IV.3 Timing of CDD Measures 17
IV.4 Enhanced Due Diligence 18
IV.5 Simplified Due Diligence 18
IV.6 Politically Exposed Persons 19
IV.7 Persons Connected to Sporting Events 19
IV.8 Application of CDD Measures to Existing Customers 19
IV.9 The Termination of the Business Relationship 20
IV.10 Reliance on Third Parties to Perform Customer Due Diligence 20
IV.11 Subsidiaries and Groups 21
V.1 Reporting Obligations 22

V.2 Prohibition of Disclosure (Tipping Off) 23
V.3 Report and Information Not Admissible 23
V.4 Power to Require Information 24
V.5 Power to Appoint an External Auditor 24
V.6 Record-Keeping 24
VI.1 Introduction 25
VI.2 A System of Internal Policies, Procedures and Controls 25
VI.3 The Appointment of the MLRO and Senior Manager 26
VI.4 Employee Screening Program and Ongoing Employee Training Program 27
VI.5 An Independent Audit Function to Test the Program 27
VI.6 Examination by the Commission 28
VII.1 Directions by the Commission 30
VII.2 Supervisory and Enforcement Measures 30
VII.2.1 Supervisory and Remedial Measures 30
VII.2.2 Disciplinary Measures 31
VII.2.3 Factors Considered by the Commission 31
VII.2.4 Urgent Protective Action 31
VII.2.5 Publication and Regulatory Notice 31
VII.3 Cooperation with Foreign Regulators and Law Enforcement 32
VIII.1 Relationship to Other Instruments 33
VIII.2 Transitional Provisions 33
VIII.3 Amendment 33
Category 1 — Prohibited Jurisdictions 36
Category 2 — High-Risk Jurisdictions (Enhanced Due Diligence Required) 36
Category 3 — Jurisdictions Subject to Monitoring 36

PART I

Application, Purpose and Functions of the Commission

1. General Statement and Purpose

The Niisitapi Gaming Commission issues this regulatory instrument to protect the integrity of gaming conducted under its authority and to ensure that licensed gaming is not used to facilitate money laundering, terrorist financing, proliferation financing, sanctions evasion, or related financial crime. The Commission requires every licensee to maintain effective, risk-based systems and controls consistent with the Financial Action Task Force (FATF) Recommendations and with all AML/CFT/CPF and sanctions laws that are legally applicable to the licensee or its activities. Compliance with this regulatory instrument is a continuing condition of licensing and forms part of the Commission's assessment of the suitability and ongoing fitness of every licensee.

2. Application

This regulatory instrument applies to all remote gaming under a License awarded by the Commission and offered from the Territory. Remote gaming under a License is offshore in nature: it must be directed only to players physically located outside the Domestic Territory and must not be offered to persons within it (Gaming Regulations, Regulation 4). Unless the Commission expressly determines otherwise in writing, each licensee is responsible for demonstrating compliance on a continuing basis. On the coming into force of this regulatory instrument:

- every B2C Licensee, being a Licensee authorized to provide gaming services directly to end-user customers ("B2C Operators") is deemed a "Reporting Entity" for the purposes of this Code of Practice;
- compliance with this Code of Practice is deemed a condition of the relevant License;
- B2B Licensees, and Suppliers approved or registered by the Commission under Regulation 33.1, in relation to services provided to B2C Operators ("B2B Suppliers") are subject to a degree of AML/CFT/CPF compliance proportionate to their service offering, as further specified by the Commission; and
- this Code of Practice is to be read together with any other guidance, standards, notices or directions issued by the Commission; in the event of any conflict, this Code of Practice shall prevail.

3. Effect

This regulatory instrument has regulatory effect within the Commission's jurisdiction and is enforceable as a condition of every License, approval, registration or authorization to which it applies (Gaming Regulations, Regulation 46.3). A licensee must comply with the substance as well as the form of these requirements and must be able to demonstrate compliance to the Commission. The Commission may rely on this regulatory instrument in licensing, supervision, examination,

remediation, disciplinary, and enforcement decisions, and may use it as a basis for cooperation and mutual assistance with competent domestic or foreign regulatory and law-enforcement authorities.

4. Legal Authority and Regulatory Status

This regulatory instrument is issued pursuant to the powers conferred on the Commission by the Online Gaming Regulations (in particular Regulation 46), together with the Commission's authority to establish License conditions, issue binding directions, supervise licensees, require information, conduct examinations, and take disciplinary or protective action in relation to licensed gaming.

This regulatory instrument also gives effect to Regulations 13.1(m) and 21 of the Online Gaming Regulations (the "Gaming Regulations") and is issued as a standard under Regulation 46 of those Regulations. It may impose requirements that are stricter than, and consistent with, the minimum in the Gaming Regulations. This Code of Practice constitutes the AML Policy referred to in the Gaming Regulations. In this Code of Practice, "licensee" corresponds to "Licensee" in the Gaming Regulations, and "B2C Operator" to "Operator" in the Commission's Responsible Gaming Policy and Player Complaints Policy.

Nothing in this regulatory instrument limits or replaces an obligation imposed by legislation that applies independently to a licensee, its directors, officers, employees, customers, transactions, or property, including, where a licensee, its customers or its transactions have a connection to another jurisdiction, the anti-money laundering, counter-terrorist financing and sanctions legislation of that jurisdiction. Where an applicable statute, regulation, court order, sanctions measure, or lawful direction imposes a stricter requirement, the stricter requirement prevails to the extent of any inconsistency.

The Commission may issue guidance, notices, technical standards, forms, reporting instructions, or written directions to explain or give practical effect to this regulatory instrument. Such instruments must be read consistently with this regulatory instrument and with the Commission's enabling legislation.

5. Functions and Powers of the Commission

In addition to the functions, duties, and powers conferred by the Gaming Regulations and any other applicable law, the Commission shall administer and supervise compliance with this regulatory instrument and may, where reasonably necessary for that purpose:

- coordinate the assessment of money laundering, terrorist financing, and proliferation financing risks in and from the Territory, and apply resources aimed at ensuring those risks are effectively mitigated;
- based on that assessment, apply a risk-based approach to ensure that measures to prevent or mitigate money laundering, terrorist financing, and proliferation financing are commensurate with the risks identified within its regulatory scope;
- issue guidance, directions and notices necessary to give practical effect to this Code of Practice; and
- periodically review and update this Code of Practice to reflect developments in the FATF Recommendations, the outcomes of any applicable national risk assessment, and lessons learned from supervisory experience.

The Commission may also, where reasonably necessary for that purpose:

- require a licensee to provide records, data, risk assessments, policies, reports, audit material, customer files, transaction information, or other information reasonably required for supervisory purposes;
- conduct or commission on-site or remote examinations, thematic reviews, file testing, interviews, and control assessments;
- require a licensee to prepare and implement a remedial action plan within a period specified by the Commission;
- impose additional License conditions or risk-mitigation measures where the Commission identifies heightened or inadequately controlled ML/TF/FP or sanctions risk; and
- take supervisory, protective, or enforcement action in accordance with Part VII and the Commission's enabling legislation.

6. Inter-Agency Cooperation

The Commission may cooperate with, and where appropriate provide information to, domestic law enforcement agencies and other domestic or international agencies concerning actual or potential money laundering, terrorist financing, or proliferation financing activity of which it becomes aware. The Commission may enter into memoranda of understanding with regulatory authorities of other jurisdictions to assist in the regulation and supervision of AML/CFT/CPF matters, provided that no such memorandum requires assistance beyond that contemplated by this Code of Practice, or relieves the Commission of its functions or duties under this Code of Practice.

7. Obligation of Confidentiality

Information received by the Commission from or about a Reporting Entity under this Code of Practice is to be treated as confidential. No person working for or on behalf of the Commission may disclose such information to any person outside the Commission except: in summary or aggregate form that does not identify the Reporting Entity; in the discharge of the Commission's disciplinary duties; in judicial review of a Commission decision; in proceedings initiated by the Commission in the exercise of its duties; or to a domestic or foreign law enforcement or regulatory agency that agrees to hold the information under an equivalent obligation of confidentiality. This Part is without prejudice to disclosures to the Regulatory Support Provider for the performance of its functions and to any other disclosure permitted by Regulation 36 of the Gaming Regulations.

PART II

Preface: Understanding the Risks

II.1 General Statements

The Commission regards effective Customer Due Diligence (CDD), ongoing monitoring, sanctions compliance, and the timely escalation and reporting of unusual or suspicious transactions as core obligations of every gaming licensee. These controls are intended to prevent a licensee, knowingly or unknowingly, from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion, or related financial crime.

This regulatory instrument establishes the minimum regulatory standards expected by the Commission. Each licensee must translate these standards into written policies, procedures, systems, controls, and governance arrangements appropriate to the nature, scale, complexity, and risk profile of its business. A failure to comply may result in supervisory or enforcement action under Part VII, without prejudice to any civil, criminal, or other liability arising under applicable law.

II.2 What is Money Laundering?

Money laundering (ML) is the process by which the proceeds of criminal activity are disguised to appear as though they originated from a legitimate source — making "dirty money look clean." It is generally understood to occur in three stages:

- Placement — the introduction of illicit funds into the financial system, for example by purchasing chips or credits for cash, redeeming value without meaningful play, funding a gaming account using credit or debit cards, prepaid instruments, or virtual assets, and then requesting a payout;
- Layering — converting the proceeds of crime into another form to disguise the audit trail, source, and ownership of funds, for example through transfers between accounts, sometimes across licensees or jurisdictions, currency exchange, or structuring of transactions;
- Integration — the re-entry of laundered funds into the legitimate economy in what appears to be an ordinary business or personal transaction, for example the purchase of luxury assets, financial investments, or commercial investments.

Money laundering is not limited to the proceeds of drug trafficking. Predicate offences include, among others, human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping, and tax crimes.

II.3 What is Financing of Terrorism?

Financing of terrorism (FT) is the financing of terrorist acts, terrorists, and terrorist organizations. A terrorist act is an act intended to intimidate a population, or to compel a government or international organization to do or abstain from doing any act. The essential difference between FT and ML lies in the origin of the funds: FT involves funds used for an illegal purpose that need not themselves be derived from criminal activity, whereas ML always involves the proceeds of crime. While ML is

primarily concerned with obscuring the source of funds, FT is primarily concerned with obscuring the ultimate use and recipient of funds.

II.4 What is Financing of Proliferation of Weapons?

Financing of proliferation (FP) is the provision of funds or financial services for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials, in breach of applicable law or United Nations Security Council resolutions.

II.5 Targeted Financial Sanctions

Targeted financial sanctions are distinct from ordinary customer-risk controls. Where sanctions legislation applies, a licensee must comply with the legal prohibitions, asset-freezing requirements, reporting duties, and restrictions imposed by that legislation. No risk-based exemption permits a licensee to transact with a person, entity, property, or activity where doing so is prohibited by applicable sanctions law.

For the purposes of this regulatory instrument, applicable sanctions legislation includes any sanctions law having binding effect in the Territory or on the relevant licensee, person, property, or transaction. Where Canadian federal sanctions law applies by operation of law, relevant instruments may include the United Nations Act and regulations made under it, the Special Economic Measures Act and its regulations and orders, the Justice for Victims of Corrupt Foreign Officials Act (Sergei Magnitsky Law) and its regulations, and the terrorist-property and listed-entity provisions of Part II.1 of the Criminal Code, together with any other binding federal sanctions measure. The Commission may identify additional legislation or official sources by notice, but such a notice does not replace the underlying law.

> **Minimum requirement.** A licensee must maintain sanctions controls proportionate to its activities and exposure. At minimum, screening must occur before or at onboarding, before permitting a withdrawal or other release of value, when material customer information changes, and promptly following relevant list updates. Screening must extend, where appropriate, to beneficial owners, controllers, authorized persons, payment counterparties, and other persons connected with the transaction. A licensee must also maintain procedures for potential-match review, escalation, false-positive resolution, freezing or blocking where legally required, and prompt reporting to the Commission and any competent authority. Where a licensee processes transactions in a foreign currency, or deals through a foreign person or financial institution, its sanctions controls must also cover the lists and rules that apply to that currency, person or institution, including asset-freezing lists and rules that treat entities majority-owned or controlled by listed persons as themselves listed. Licensees should build their sanctions compliance program around five components: management commitment, risk assessment, internal controls, testing and auditing, and training.

Where a confirmed or reasonably suspected sanctions match is identified, the licensee must not complete a prohibited transaction or make funds, property, gaming value, winnings, or economic resources available contrary to applicable law. The licensee must preserve relevant property and records, avoid tipping off where prohibited, and seek legal or regulatory direction where the legal status of the property or transaction is uncertain.

Licensees are responsible for monitoring authoritative legal sources and maintaining current screening data. Consolidated or commercial sanctions lists may be used as operational tools, but they do not replace the applicable statute, regulation, order, or official designation. The Commission may publish links, notices, or implementation guidance to assist licensees, but responsibility for legal compliance remains with the licensee.

PART III

The Risk-Based Approach

III.1 What is the Risk-Based Approach?

An AML/CFT/CPF compliance program is an essential component of a licensee's overall compliance regime. The primary goal of any such program is to protect the licensee against misuse for money laundering, terrorist financing, and proliferation financing, and to ensure full compliance with applicable law and this Code of Practice.

Based on the FATF Recommendations, licensees are required to apply a Risk-Based Approach (RBA) when designing policies, procedures, and controls. An RBA allows a licensee to ensure that measures to prevent or mitigate risk are commensurate with the risks identified: the higher the risk, the more extensive the measures required; where risk is lower, simplified measures may be applied, provided this is consistent with any applicable national risk assessment.

Applying a Risk-Based Approach requires a licensee to:

- assess, in advance, the risk that money laundering, terrorist financing, or proliferation financing may occur within its organization;
- design and implement appropriate policies, procedures, and controls to manage and mitigate the identified and assessed risks;
- monitor and improve the effective operation of those policies, procedures, and controls; and
- document its risk assessments, including everything done and the reasoning for it, and make this available to the Commission on request.

III.2 The Business and Customer Risk Assessments

The foundation of the risk-based approach is the risk assessment a licensee carries out of its own operations. This requires an understanding of the risk to which the business is generally exposed (the Business Risk Assessment), as well as an assessment of the risk posed by each individual customer (the Customer Risk Assessment).

III.2.1 Business Risk Assessment (BRA)

All licensees must carry out a Business Risk Assessment to identify the ML/TF/FP risks to which they are exposed, and to ensure that the policies, controls, and procedures adopted are adequate to prevent and mitigate those risks. The BRA should address the ways in which the licensee's products and services could be used to launder money, finance terrorism, or finance proliferation, and the extent of that risk. The BRA is an enterprise-wide assessment proportionate to the nature, scale and complexity of the licensee’s business. Special consideration must be given to the type of customers, products and services offered, transactions, payment methods, delivery channels, technology, outsourcing arrangements, and geographic risk factors, and the BRA should incorporate the outcomes and recommendations of any applicable national risk assessment and any AML/CFT priorities

published by the Commission or the Niisitapi Sovereign Bank (NSB), acting as financial intelligence unit (FIU).

Once business risk has been assessed, the licensee may set a risk appetite — deciding how much risk it is prepared to accept — which assists in establishing and maintaining its compliance program. Licensees must revise the BRA whenever there is a material change to their environment or business activities, such as the introduction of new payment methods, new markets, new games, or regulatory changes, and in any event at least once a year. The BRA must be documented and approved by the licensee's Governing Body, made available to the Commission on request, and must cover:

- the methodology adopted;
- the reasons for considering a given risk factor as low, medium, or high risk;
- the outcome of the BRA; and
- any information sources used.

III.2.2 Customer Risk Assessment (CRA)

A customer-specific risk assessment must be carried out either prior to an occasional transaction or during the establishment of a business relationship, and may need to be revised at a later stage, resulting in an adjustment to the customer's risk rating. The CRA assesses the particular risk the licensee is exposed to in providing services to a given player, and the information collected forms the customer's risk profile. On the basis of the CRA, the appropriate level of CDD is applied as stipulated in the licensee's Customer Acceptance Policy (CAP). The CAP must provide:

- a description of the type of players likely to pose a higher-than-average risk of ML/FT/FP;
- the risk indicators presenting low, medium, or high risk;
- the level of CDD measures, including ongoing monitoring, to be applied at each level; and
- the circumstances under which service to a customer will be declined or terminated.

In drawing up the CAP, the licensee must comply with its obligations regarding Politically Exposed Persons and sanctions screening, set out in Part IV below.

III.2.3 Risk Factors Specific to the Gaming Sector

At minimum, both the BRA and CRA must address the four risk areas below. The BRA must also address the additional risks in (e).

(a) Customer Risk

Customer risk is the risk of ML/TF/FP arising from maintaining a relationship with a given person. Categories of customer whose activity may indicate a higher risk include:

- customers with multiple sources of income;
- customers with irregular income streams;
- Politically Exposed Persons (PEPs);
- high spenders whose funds may plausibly derive from illegal activity;
- disproportionate spenders, whose spending is inconsistent with the licensee's information about their known source of income or assets;
- casual customers, particularly where a spending pattern changes materially;
- improper use of third parties, where criminals use others to gamble, to break up large amounts of cash, or to buy chips or credits or cash out on their behalf to avoid CDD;

- customers using multiple accounts to hinder the licensee's ability to track their activity;
- unknown customers redeeming large amounts of credits; and
- junket-style arrangements, where an intermediary monitors player activity and collects on credit extended to players.

A customer having a single, regular, and verifiable source of income poses less risk than a customer with multiple or irregular income streams; licensees should set a value representing the upper bound of a typical player's transactions and treat material deviations as a risk indicator.

(b) Geographic Risk

Geographic risk is the risk posed by the customer's nationality, residence, place of birth, and source of wealth. Countries with weak AML/CFT frameworks, significant levels of corruption, exposure to international sanctions, or known terrorist activity are to be treated as high risk. Licensees should consult a range of sources when compiling their own list of higher- and lower-risk jurisdictions, including:

- countries on FATF's list of High-Risk Jurisdictions subject to a Call for Action;
- countries on FATF's list of Jurisdictions under Increased Monitoring;
- countries identified by FATF-style regional bodies in a public statement;
- countries identified as jurisdictions of concern in recognized international narcotics or financial-crime reporting;
- countries identified by the European Commission (or an equivalent body) as having strategic AML/CFT deficiencies;
- jurisdictions, institutions or classes of transactions designated by a competent foreign authority as being of primary money laundering concern, or described in official advisories on high-risk jurisdictions;
- countries subject to sanctions by OFAC or an equivalent sanctions authority; and
- countries ranked poorly on a recognized corruption-perceptions index.

Licensees must maintain a documented list of jurisdictions considered high risk and those considered low risk, and must review this list at least quarterly. A working template for a jurisdiction-restriction list is provided at Annex 2.

(c) Product, Service, and Transaction Risk

Some products and services are inherently riskier than others and more attractive to criminals, including those allowing a customer to influence the outcome of a game individually or in collusion with others. High-risk factors include:

- proceeds of crime — risk that transferred funds derive from illegal activity such as payment-card fraud, narcotics trafficking, or theft from an employer;
- cash — used to exchange large amounts of illicit proceeds in small denominations for larger ones;
- anonymous payment methods, such as prepaid cards and virtual assets;
- use of gaming accounts for purposes other than gambling, including deposit-and-withdraw patterns with minimal play;
- game types especially conducive to structuring (for example, even-money bets);
- peer-to-peer gaming;
- use of accounts or cards issued in the name of third parties;
- transfer of funds from one gaming account to another;

- credit or marker facilities, currency exchange, and check cashing;
- multiple accounts or wallets, particularly where an operator owns or controls multiple platforms;
- changes to the financial institution account used to fund a gaming account;
- identity fraud, including the use of stolen financial-account details or stolen identities to open accounts;
- use of cash to fund a prepaid card, which poses risks similar to cash itself;
- games involving multiple operators, such as poker on a shared platform; and
- electronic wallets not licensed in a reputable jurisdiction, or that accept cash deposits, or that may obscure the underlying transaction to the casino from the customer's bank statement.

Licensees must maintain a documented list of products, services, and payment methods considered high risk.

(d) Distribution Channel Risk

The channel through which a business relationship is established, or through which transactions are carried out, affects the risk profile of that relationship. Channels favouring anonymity increase risk absent mitigating measures; non-face-to-face interaction is to be treated as a high-risk factor unless the licensee adopts technological measures addressing the heightened risk of identity fraud or impersonation; and the involvement of a third party in the customer relationship increases risk, particularly where that third party is not itself subject to AML/CFT obligations.

(e) Payment-Method, Technology and Outsourcing Risk

The BRA must also address the risks arising from the payment methods a licensee accepts and pays out through; from the technology used to deliver or support its services (see Part III.3); and from outsourcing and reliance on suppliers, agents, and group companies, which do not reduce the licensee's own responsibility (Part IV.10 and Gaming Regulations, Regulations 13.8 and 33).

III.3 Technological Developments Risk Assessment

A licensee must maintain procedures and controls to prevent the misuse of technological developments for money laundering or terrorist financing, and must identify and assess the risk that may arise whenever a new product is developed, a new business practice emerges, a new delivery mechanism becomes available, or a new or developing technology is applied to new or pre-existing products. Such a risk assessment must take place prior to launch, must be documented, and any identified risk must be mitigated before the innovation is deployed.

PART IV

Customer Due Diligence

IV.1Introduction

Licensees are prohibited from keeping anonymous accounts or accounts in obviously fictitious names. A licensee must identify the player and obtain the player's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge of the customer, a licensee may not establish or maintain a business relationship, or carry out an occasional transaction. A sound CDD program is the primary means of preventing money laundering, terrorist financing, and proliferation financing.

The customer's risk profile allows a licensee to apply a level of CDD commensurate with the identified ML/TF risk, and provides documentation to assess the risk associated with the player and to build a customer profile against which unusual behaviour can be detected. Any unusual behaviour must be escalated to the MLRO and, where reportable under Part V.1, reported to the NSB.

A licensee must undertake CDD measures where:

- a customer engages in a single financial transaction, or in linked financial transactions, equal to or above the CDD Threshold of EUR 3,000 (or the equivalent in another currency), as set by this Code of Practice (Gaming Regulations, Regulation 21.11);
- an occasional transaction is carried out at or above the CDD Threshold;
- there is a suspicion of money laundering or terrorist financing, irrespective of any threshold; or
- the licensee has doubts about the veracity or adequacy of previously obtained customer identification data.

Where a licensee carries out an occasional transaction at or above the CDD Threshold, it remains obliged to apply CDD measures. Licensees are also subject to this obligation where they execute a series of linked transactions that, though individually below the CDD Threshold, together meet or exceed it. Transactions are considered linked where they are carried out by the same player through the same game, within one gaming session, or within one gaming day (as described in Part V.1). A licensee’s documented AML/CFT/CPF policies may set earlier or additional triggers, including on a cumulative basis over the relationship (Gaming Regulations, Regulations 21.1 and 21.6).

Use of Physical Establishments

Where an online licensee makes use of a physical establishment to extend its customer reach, the interaction between the customer and the licensee remains a business relationship subject to this Code of Practice. The licensee must ensure the physical establishment applies the licensee's own AML/CFT/CPF policies and procedures, must identify and verify the operator of the establishment and satisfy itself that the operator is of good standing, and must monitor activity conducted through the establishment's account on an ongoing basis to ensure compliance. All measures taken to ensure such compliance must be documented.

IV.2 The CDD Measures

At minimum, CDD comprises the following measures:

- identifying the player and verifying that player's identity using reliable, independent source documents, data, or information;
- identifying the beneficial owner, and taking reasonable measures to verify their identity such that the licensee is satisfied it knows who the beneficial owner is, including, for legal persons and arrangements, understanding the ownership and control structure of the customer;
- understanding, and as appropriate obtaining information on, the purpose and intended nature of the business relationship; and
- conducting ongoing due diligence on the business relationship and scrutiny of transactions throughout its course, to ensure that transactions are consistent with the licensee's knowledge of the player, their business, and their risk profile, including, where necessary, their source of funds.

A licensee, its directors, officers, and employees are prohibited from disclosing that a report has been or is being made to the NSB. Where the licensee has a suspicion that transactions relate to ML or TF, it should take into account the risk of tipping off when performing further CDD; if the licensee reasonably believes that performing further CDD will tip off the player, it may decline to pursue that process and should instead file a report.

IV.2.1 Identification and Verification of the Player

Identification refers to the collection of the player's personal details; verification consists of confirming those details using reliable, independent source documents, data, or information. The extent of information required, and the extent of verification, will vary with risk.

At minimum, when identifying the player, the following must be collected: full name; permanent residential address; date of birth; place of birth; nationality; identity document number; and, where one has been issued to the player, a tax identification number or equivalent national identifier. In low-risk scenarios, a licensee may limit identification to name, address, and date of birth; in high-risk situations, a licensee should consider collecting additional personal details.

Verification is ordinarily carried out against an unexpired, government-issued document bearing a photograph (such as a passport or national identity card). Where such a document does not permit verification of residential address, the licensee may obtain alternative documentation such as a bank statement, utility bill, letter from a public authority, or rental agreement no older than six months. A licensee may also verify information by contacting the player by letter, email, or telephone, by sending a verification code, by checking social media, telephone directories, company registries, or media sources, and by using biometric checks to confirm that the individual presenting a document is the person described in it. A licensee may also cross-reference the information in its possession against geo-location data, IP address data, and funding-method data.

The Commission’s Responsible Gaming Policy (section 6.3) requires verification against a valid government-issued identity document when the applicable thresholds are reached and, in every case, before the first withdrawal. The alternative and supplementary methods described in this Part, and simplified CDD under Part IV.5, do not replace that requirement.

Verification implies checking that the document presented is legitimate and has not been stolen from its true owner. Extra care should be taken where foreign documentation is presented, particularly where the document type is unfamiliar. Where the licensee does not have sufficient comfort that it

knows its player, it should take additional measures, such as requesting additional identification documents, requesting a photo of the player holding the identification, requiring an initial payment through an account held in a reputable jurisdiction, or using a system that generates a code for transmission to a verified mobile number.

All players must be screened against applicable sanctions lists and assessed for PEP status before, or at, the point of first business, and the licensee must ensure it does not do business with a sanctioned customer.

IV.2.2 Identification and Verification of the Beneficial Owner

Licensees must ensure customers are registering to play and transact on their own behalf, for example through explicit terms and conditions and a declaration accepted by the registering player. Licensees are not expected to rely on this declaration alone, and must have ongoing procedures capable of detecting instances where a player is in fact playing on behalf of a third party.

While most licensees will not typically encounter beneficial-ownership situations, these cannot be excluded — for example, where funds wagered by a player are collected from multiple persons who will share in any winnings (a syndicate). In such cases, those persons are to be treated as beneficial owners and identified and verified accordingly. Where a licensee's business model includes corporate accounts used to hedge exposure, the applicable beneficial-ownership requirement relates to the beneficial owners of the corporate entity.

For corporate customers, the licensee must obtain satisfactory evidence to identify business participants, and must take reasonable steps to verify the identity of any person holding 25% or more of the shares or voting rights, or who otherwise exercises ultimate effective control. Where no natural person is identified on this basis, the natural person holding the position of senior managing official should be identified instead. In every case, the licensee must also identify at least one natural person with significant responsibility to control, manage or direct the corporate customer, for example a chief executive, chief financial officer, managing member or general partner.

IV.2.3 Purpose and Intended Nature of the Business Relationship

Although the purpose behind opening a gaming account is generally self-evident, CDD still requires the development of a customer risk profile sufficient to detect unusual activity in the course of the relationship. Licensees must collect sufficient information, and where necessary documentation, to establish a customer's source of wealth and expected level of activity. Where risk is not high, a declaration from the customer with some supporting detail (nature of employment, usual income, and similar) may suffice, and social media may also be used as a source. Where risk is higher, or the licensee has doubts about the veracity of information collected, that information must be substantiated by independent and reliable documentation.

Licensees may also develop behavioural models based on statistical data — for example, average national or disposable income data — to gauge a customer's activity, rather than collecting individual source-of-wealth information, provided their customer base is wide enough to support an average profile. This alternative is incompatible with high-risk situations, in which source-of-wealth information must still be collected.

IV.2.4 Ongoing Monitoring

A licensee must conduct ongoing due diligence on the business relationship and scrutinize transactions throughout its course to ensure consistency with its knowledge of the customer, their business, and their risk profile.

Ongoing monitoring of identity: the licensee should hold accurate and up-to-date identification data, and should be able to demonstrate that changes in identity will be detected and re-evidenced — for example by refreshing data upon key events such as a change of payment instrument, or by tracking and refreshing expiring identity evidence.

Ongoing monitoring of transactions: transaction monitoring exists to prevent involvement in ML/TF and to safeguard the licensee's reputation. Where a customer's transactions are inconsistent with what the licensee knows or expects, the licensee must question the activity and, where necessary, establish the source of the funds involved, and must decide whether the transaction is unusual and reportable to the NSB. The level of ongoing monitoring depends on the customer's risk profile, but a degree of oversight must occur even in low-risk relationships.

IV.3 Timing of CDD Measures

A licensee provides services allowing a customer to wager a stake of monetary value in a game of chance, doing business with individuals acting in their own name and on their own behalf by opening an account or club membership — a relationship expected to have an element of duration, and therefore a business relationship. Verification of identity must be conducted when a customer engages in a single financial transaction, or in linked financial transactions (Part IV.1), equal to or above the CDD Threshold; this implies all CDD measures must be completed once that threshold is reached. Verification against a government-issued identity document must in every case be completed before the first withdrawal (Responsible Gaming Policy, section 6.3).

Licensees are nonetheless required to apply a minimum level of CDD prior to reaching the threshold: at the point of opening an account, the licensee must collect at minimum name, permanent residential address, and date of birth (the minimum requirement for low-risk relationships), and must conduct PEP status and sanctions screening. The threshold is assessed on each transaction and on linked transactions as described in Part IV.1, including any peer-to-peer transfers.

Customers may continue using their gaming account while the licensee obtains outstanding information. However, if the threshold is reached because of a deposit, the player may not deposit further funds or withdraw pending completion of CDD, though may continue to play with funds already in the account. If the threshold is reached because a withdrawal is requested, the account must be frozen entirely.

If requested information is not received within 30 days of the threshold being reached, the licensee must terminate the relationship with the player. Where a presumption of money laundering or terrorist financing exists, the transaction must be reported to the NSB; where no such presumption exists, funds should be returned to the account or wallet from which they originated. Where a presumption exists, the licensee's internal procedures should determine whether funds are to be blocked, taking into account the risk of tipping off the customer.

Any hold, freeze or restriction under this Part must be objectively justified, documented, and limited to the period reasonably necessary. Unless disclosure is prohibited by law (Part V.2), the licensee must

tell the player what information is required, by when, and the reason for the delay. Once CDD and all other required checks are complete, a withdrawal of cleared funds must be processed within five working days, unless exceptional circumstances justify a longer, documented period (Gaming Regulations, Regulations 19.7 and 19.13).

IV.4 Enhanced Due Diligence

A risk-based approach requires more thorough checks for higher-risk customers. Enhanced Due Diligence (EDD) must be consistent with the risks identified, and in particular must increase the degree and nature of monitoring so as to determine whether transactions or activities appear unusual. EDD must be conducted where risk is higher, including in relation to: residents of higher-risk geographic areas; PEPs; products or transactions favouring anonymity; and new products, business practices, delivery mechanisms, or technologies. EDD measures include:

- obtaining additional information on the customer, such as occupation, previous address, and information available through public databases or the internet;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on source of funds or source of wealth — examples include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances, gifts, and compensation from legal rulings;
- obtaining information on the reasons for an intended or performed transaction;
- obtaining senior management approval to commence or continue the relationship;
- conducting enhanced monitoring of the business relationship; and
- requiring the first payment to be made through an account in the customer's name held with an institution subject to similar CDD standards.

In higher-risk situations, source-of-funds information should be requested periodically even absent any change in the customer's transaction pattern.

IV.5 Simplified Due Diligence

Where the risk of ML/TF is lower, a licensee may conduct simplified CDD measures reflecting the nature of that lower risk, for example:

- limiting identification to name, address, and date of birth where risk assessment indicates low risk;
- verifying the identity of the customer and beneficial owner after the relationship is established;
- adapting the extent of verification to the perceived risk, including reliance on alternative reputable sources even where they lack photographic evidence;
- limiting the extent of personal details verified beyond the basic identification data;
- reducing the frequency of periodic identification updates; and
- reducing the degree of ongoing monitoring, based on a reasonable monetary threshold.

Simplified CDD is never acceptable where there is suspicion of money laundering or terrorist financing, or where a specific higher-risk scenario applies. Simplified CDD does not displace the CDD Threshold or the government-issued document requirement before the first withdrawal (Responsible Gaming Policy, section 6.3).

IV.6 Politically Exposed Persons

In relation to a customer or beneficial owner who is a PEP, whether foreign or domestic, a licensee must, in addition to standard CDD:

- have appropriate risk-management systems in place to determine whether the customer or beneficial owner is a PEP;
- obtain senior management approval to establish or continue the business relationship, or to conduct an occasional transaction, with that PEP;
- take reasonable measures to establish the source of wealth and source of funds, and determine whether the player's spending pattern matches the player's stated and verified source of funds; and
- conduct enhanced ongoing monitoring of the relationship.

A "Politically Exposed Person" means an individual who holds, or has held, a prominent public function domestically, in a foreign country, or in an international organization, including a head of state or government, a government minister or equivalent senior politician, a senior government official, a senior judge, a governor of a central bank, a senior military officer, a senior diplomatic representative, and a board chair, chief executive, or chief financial officer of a state-owned enterprise or comparable body. These requirements extend to immediate family members (spouse, de facto partner, children and their spouses or partners, parents, siblings, and the parents and siblings of the spouse or de facto partner) and close associates (persons known to jointly or solely beneficially own a legal entity or arrangement with the PEP, and persons widely and publicly known to maintain an unusually close personal or professional relationship with the PEP, including a person in a position to conduct substantial financial transactions on the PEP’s behalf) of a PEP.

PEP screening must be carried out at onboarding and must be repeated regularly during the business relationship. Where a player who was not identified as a PEP at onboarding subsequently becomes one, the licensee must apply the measures above within 30 days of becoming aware of that status, failing which the relationship must be terminated.

IV.7 Persons Connected to Sporting Events

Where a licensee accepts wagers on a sporting event, team, or organization, it must, in addition to standard CDD, maintain risk-management systems to determine whether a customer, or an immediate family member or close associate of a customer, has a close connection to that sport, team, or event — for example by owning, playing for, coaching, training, or managing a team, or holding a senior role with the sport's Governing Body. Where such a connection is identified, the licensee must obtain senior management approval to establish or continue the relationship, take reasonable measures to establish source of wealth and source of funds, and conduct enhanced ongoing monitoring, on the same basis as for a PEP under Part IV.6.

IV.8 Application of CDD Measures to Existing Customers

Licensees must apply CDD measures to existing customers on the basis of materiality and risk, and must conduct due diligence on existing relationships at appropriate times. Where existing procedures are sufficient to meet the obligations of this Part, a licensee may continue applying them, paying

particular attention to ongoing-monitoring obligations. Where a licensee had no adequate procedures in place, it must apply CDD on a risk-sensitive basis to its existing book of customers.

IV.9 The Termination of the Business Relationship

Where the obligations arising from CDD cannot be met, the licensee may not establish, or must terminate, the business relationship or transaction, and must keep a record of all attempts made to obtain the necessary information. The licensee may either close the account or keep it blocked and suspended. Where a customer later provides the requested information following closure or suspension, the licensee must consider whether the delay affects the ML/TF risk associated with the relationship.

A customer's reluctance to provide CDD information should not automatically be equated with suspicion of ML/TF/FP; the licensee must weigh all available information. Where a presumption of ML/TF/FP nonetheless exists, the licensee must submit a report to the NSB. Where there is no basis for retaining funds, they must be returned to the player through the same channel by which they were received.

IV.10 Reliance on Third Parties to Perform Customer Due Diligence

A licensee may rely on a third party to perform the identification and verification, beneficial-owner and purpose-and-nature elements of the CDD measures set out in Part IV.2, provided the following criteria are met:

- the licensee obtains the relevant CDD information from the third party immediately upon relying on it;
- the licensee has an agreement with the third party ensuring that copies of identification data and other relevant documentation will be made available on request, tested periodically to confirm this arrangement functions as intended (the licensee remains responsible for the customer risk assessment, PEP determination, and ongoing monitoring);
- the licensee satisfies itself that the third party is regulated, supervised, or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements comparable to this Code of Practice; and
- the licensee has regard to available information on country risk when determining which jurisdictions a relied-upon third party may be based in.

This differs from an outsourcing or agency arrangement, in which the outsourced entity applies CDD on the licensee's behalf and in accordance with the licensee's own procedures, under the licensee's control. Any activity performed by an agent or group company is treated as performed by the licensee itself, and the licensee remains responsible at all times for ensuring the agent's or group company's compliance with its AML/CFT/CPF controls. The decision whether to onboard, or to continue a relationship with, a customer may never itself be outsourced.

IV.11 Subsidiaries and Groups

Where a licensee relies on a third party that is a related company or part of the same corporate group, and that group applies a program combating ML/TF/FP risk and is supervised by a competent authority of another jurisdiction to a standard equivalent to this Code of Practice, the Commission may consider the licensee adequately controlled by that group-wide program. Where the group program does not impose equivalent requirements, the licensee must apply measures equivalent to those required by this Code of Practice, to the extent permitted by the law of the relevant third country. Where the law of that third country does not permit equivalent measures, the licensee's parent entity must inform the Commission and take additional measures to effectively mitigate the resulting risk.

PART V

Reporting, Confidentiality and Record-Keeping

V.1 Reporting Obligations

Licensees must maintain adequate procedures covering the recognition, documentation, and reporting of unusual or suspicious transactions, whether completed or merely intended. An unusual transaction is one inconsistent with the player's profile; the first key to recognizing that a transaction is unusual is therefore knowing enough about the player, which is the purpose of the CDD obligations in Part IV.

Management must provide staff with specific guidance and training in recognizing and adequately documenting unusual transactions. All such transactions must be reported internally to the MLRO in the format approved by management, together with supporting documentation such as copies of identification documents and cash-out records. The MLRO must maintain an adequate filing system for these records, and where an internally reported transaction is not escalated externally, the reasons must be documented and signed off by the MLRO or management.

In line with the FATF Recommendations on ongoing due diligence and on reporting suspicious transactions (Recommendations 10 and 20), licensees must pay special attention to all complex or unusually large transactions, and all unusual patterns of transactions, that have no apparent economic or lawful purpose. At minimum, the following are deemed unusual or reportable:

- a transaction reported, or proposed for report, to police or judicial authorities in connection with money laundering or terrorist financing;
- a transaction by or on behalf of a natural or legal person, group, or entity named on a list adopted under applicable sanctions legislation;
- a transaction, or series of linked transactions, of EUR 10,000 or more, within a single gaming day, regardless of payment method, including a cashless transfer, the acceptance or release of a deposit, the sale of chips or credits, or a cash-out at or above that threshold; and
- a transaction for which there is cause to presume a connection to money laundering, terrorist financing, or proliferation financing.

A transaction may be a single transaction or a series, combination, or pattern of transactions cumulatively meeting the reporting threshold, considered per gaming day (or such other period as the Commission may specify). “Gaming day” means the 24-hour accounting period the licensee uses for its business, which the licensee must fix, document and disclose to the Commission. Inflows (deposits and purchases of credits) and outflows (withdrawals and payouts) must be aggregated separately for each player and each gaming day. Before a transaction that meets the reporting threshold is completed, the licensee must identify and verify the person conducting it and any person on whose behalf it is conducted, and a threshold report must be filed with the NSB within 15 calendar days after the gaming day on which the threshold is met. Structuring, meaning conducting or attempting transactions in a manner designed to evade a threshold, identification or recordkeeping requirement of this Code of Practice (for example by splitting transactions or using multiple accounts, wallets or payment methods), is an indicator of suspicion that must be escalated to the MLRO, whether or not any single transaction reaches a threshold.

By virtue of this Code of Practice, a licensee must report an unusual or intended unusual transaction to the NSB without delay, and in any event within 5 business days of forming the relevant suspicion where the matter concerns money laundering or another predicate offence, or within 24 hours where the matter concerns terrorist financing. Reports must state the grounds for the suspicion, and licensees must document the reasoning behind any decision to report, or not to report, a matter. Where a matter requires immediate attention, such as an ongoing money laundering scheme or suspected terrorist financing, the licensee must also notify the NSB, and where appropriate a law-enforcement authority, immediately by telephone or other urgent channel, in addition to filing the written report. Where suspicious activity continues after a report has been filed, the licensee must review the relationship on a risk basis (as a guide, at least every 90 days) and file a further report covering the continuing activity.

Each licensee must register with the NSB and, where the reporting authority operates a portal or bulk-reporting facility, obtain access to it following validation. Reports and supporting documentation should be submitted in English. A licensee and its directors, officers, and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting in good faith to the NSB.

A suspicious transaction or activity is reportable irrespective of its value where applicable law so requires (Gaming Regulations, Regulation 21.3). Where lawful, a licensee must preserve the records, account data, communications and transaction information associated with a suspicious matter; must implement any lawful freeze, restraint, rejection, monitoring or other direction issued by a competent authority; and must cooperate fully with the NSB, the Commission, the Regulatory Support Provider and law-enforcement authorities.

V.2 Prohibition of Disclosure (Tipping Off)

A licensee and its senior management and employees must not disclose to a customer or to any third party any details or information connected with a report filed with, or a request for information made by, the NSB. This restriction exists so as not to jeopardize an analysis or investigation. Caution is advised when a licensee considers terminating a relationship or blocking transactions following a report; drastic action should be taken only where there is no reasonable alternative, since unjustified action may alert the player. In such circumstances, it is generally preferable to increase ongoing monitoring and submit further reports on any additional suspected instances of ML/TF/FP. These restrictions apply equally when a licensee responds to a player complaint, provides records to an alternative dispute resolution entity, or otherwise communicates with a player (see the Commission's Player Complaints Policy).

V.3 Report and Information Not Admissible

In any court, tribunal, or disciplinary proceeding, neither an unusual or suspicious transaction report, nor any document purporting to set out information contained in such a report (including the formation or existence of a suspicion), nor evidence of whether a document or information was produced to the Commission or the NSB in relation to such a report, is admissible.

V.4 Power to Require Information

The Commission may, by written notice, require a licensee to provide specified information or documents, or to attend before an officer of the Commission and answer questions, within such reasonable time and at such place as may be specified. Information held in a computer or other storage medium, or recorded otherwise than in legible form, must be produced in legible form or in a form from which legible information can readily be produced.

V.5 Power to Appoint an External Auditor

Where the Commission has reasonable cause for concern regarding a licensee's compliance with this Code of Practice, it may appoint a suitably qualified person to audit the licensee's compliance, at the licensee's expense.

V.6 Record-Keeping

Licensees must maintain, for at least five years, all necessary records of transactions (both domestic and international) sufficient to permit the reconstruction of individual transactions, including the amounts and types of currency involved, so as to provide evidence for the prosecution of criminal activity if required.

All records obtained through CDD — including copies of official identification documents, account files, and business correspondence — must be kept for at least five years after the business relationship ends, or after the date of an occasional transaction. CDD information and transaction records must be made available to the Commission and other competent domestic authorities upon lawful request. A licensee must provide the Commission with a copy of all specified records whenever it relocates its business or ceases operations.

Records of CDD, sanctions and PEP screening, transaction monitoring, investigations of unusual transactions, risk assessments, and AML/CFT/CPF decisions (including decisions not to report), together with internal reports and training records, must also be kept for at least five years after the end of the business relationship or the relevant transaction, or for any longer period required by law or by a competent authority (Gaming Regulations, Regulation 21.10). A licensee must also keep a copy of every report filed with the NSB, together with the supporting documentation, for at least five years from the date of filing. Supporting documentation is treated as filed with the report and must be produced on request to the NSB, the Commission or a law-enforcement authority.

Voluntary information sharing. Licensees may share information with one another, and with the NSB, about persons and transactions that may involve money laundering, terrorist financing or proliferation financing, provided that each licensee has first notified the Commission of its participation, has taken reasonable steps to confirm that the other licensee also participates, uses the information only to identify and report suspected ML/TF/FP, to decide whether to open or maintain an account, or to meet its AML/CFT/CPF obligations, and keeps the information secure and confidential. A licensee must respond to an information request from the NSB within the period the request specifies.

PART VI

Anti-Money Laundering, CFT and CPF Compliance Program

VI.1 Introduction

An AML/CFT/CPF compliance program is an essential component of a licensee's compliance regime. Its primary goal is to protect the organization against money laundering, terrorist financing, and proliferation financing, and to ensure full compliance with applicable laws and regulations; designing, structuring, and implementing this program should be a top priority for every licensee.

The basic elements every licensee must address in its compliance program are:

- a system of internal policies, procedures, and controls;
- a designated MLRO with day-to-day oversight of the program, a designated senior manager (a Key Person other than the MLRO), and a Governing Body that retains ultimate accountability;
- an employee screening program and an ongoing employee training program; and
- an independent audit function to test the program.

The program must also ensure that obligations regarding CDD, reporting of unusual transactions, retention periods, data protection, and training are met. It must be tested systematically and adapted to the current risks arising within the licensee's own organization, and must have the approval of the Governing Body. Licensees must ensure that any foreign branches or subsidiaries implement AML/CFT/CPF measures consistent with the requirements of the Territory.

VI.2 A System of Internal Policies, Procedures and Controls

Every licensee must maintain policies and procedures, including a policy statement clearly expressing senior management's commitment to combat the abuse of its facilities, products, and services for money laundering, terrorist financing, and proliferation financing. These policies must state the licensee's intention to comply with applicable AML/CFT/CPF legislation and this Code of Practice, in particular regarding CDD, the reporting of unusual transactions, and record-keeping, and must set the tone for the organization.

Standard operating procedures translate policy into acceptable and workable practice, and must be more detailed than the policies themselves. Licensees must have a process in place to stay abreast of regulatory change, keeping the program current. The program also relies on a variety of internal controls enabling the MLRO to recognize deviations from standard procedures and protocols. All AML/CFT/CPF policies and procedures must be in writing, approved by the Governing Body, and communicated to employees. Procedures must set out how the licensee uses all available information, including account, payment, device, geolocation and gaming-session data, to determine when identification information must be obtained and verified, whether a transaction or pattern of transactions is reportable, and whether any record must be made and retained, and must make use of automated monitoring where the licensee’s systems allow. A licensee must also maintain a confidential internal channel through which employees can report suspected breaches of its

AML/CFT/CPF controls or suspicious activity to the MLRO or the Governing Body, and must not retaliate against anyone who reports in good faith.

VI.3 The Appointment of the MLRO and Senior Manager

From the commencement of operations, each licensee must appoint a Money Laundering Reporting Officer (MLRO): a senior officer at management level, independent from gaming operations, responsible for the detection and deterrence of money laundering and terrorist financing. The MLRO must be a different individual from the Compliance Officer appointed under the Gaming Regulations (Regulations 13.5 and 21.5), and must not be a director of the licensee. The MLRO must have sufficient expertise, authority, resources and independence, timely access to customer identification data, other CDD information, transaction records, and other relevant information, and direct access to senior management and the Governing Body, and must be readily accessible to, and subject to the supervision of, the Commission and the NSB. At minimum, the MLRO is responsible for:

- designing and implementing the compliance program;
- verifying adherence to applicable laws and regulations regarding the detection and deterrence of ML/TF/FP;
- reviewing compliance with the licensee's own policies and procedures;
- organizing staff training on compliance-related issues;
- analyzing transactions and determining whether they are reportable under the applicable indicators;
- reviewing all internally reported unusual transactions for completeness and accuracy;
- keeping records of internally and externally reported unusual transactions;
- designing an internal procedure for when a report of an unusual transaction will lead to blocking or freezing of an account, taking into account the risk of tipping off;
- conducting closer investigation of unusual transactions where necessary;
- preparing external reports of unusual transactions;
- making necessary changes to the compliance program;
- remaining informed on local and international ML/TF/FP developments and proposing improvements to management;
- preparing periodic information on the licensee's efforts against ML/TF/FP for senior management; and
- reporting to the Governing Body at least annually, as set out below.

These responsibilities must be included in the MLRO's job description, which must be signed and dated by the officer indicating acceptance of the entrusted responsibilities. A working template job description is provided at Annex 5.

Senior manager. In addition to the MLRO, the licensee must designate a suitably qualified senior manager, who must be a Key Person other than the MLRO, with responsibility for implementing and overseeing the AML/CFT/CPF framework (Gaming Regulations, Regulation 21.4). The Governing Body retains ultimate accountability for AML/CFT/CPF compliance.

Annual report to the Governing Body. The MLRO must report to the Governing Body at least annually on material AML/CFT/CPF risks, the effectiveness of controls, significant incidents, suspicious-activity reporting, training, remediation, and the current enterprise-wide risk assessment. Material issues must be escalated without waiting for the annual report.

Notification to the Commission. The appointment, replacement, resignation or removal of the MLRO, who is a Key Person, must be notified promptly to the Commission and is subject to any suitability or approval requirements the Commission prescribes (Gaming Regulations, Regulations 13.1(q) and 21.4).

VI.4 Employee Screening Program and Ongoing Employee Training Program

Licensees must ensure that their business is conducted to a high ethical standard and that applicable laws and regulations relating to financial transactions are followed, and must establish and adhere to proper policies and procedures for screening employees for relevant criminal records prior to hire, upon transfer or promotion into a position of trust, and where an employee's role, risk, or circumstances materially change.

Licensees must develop and provide training to all personnel who handle transactions that may be flagged as unusual, addressing at minimum the following, calibrated by role:

- New employees — general training on the nature and process of ML/TF/FP, the need to report unusual transactions to the designated officer, the licensee's internal policies and procedures, and applicable ML/TF/FP methods and trends in the gaming sector, together with an explanation of CDD and the objective and subjective indicators used for reporting;
- Dealers, cashiers, and gaming-floor or player-support personnel — the front line of defence, requiring a general course on the importance of AML controls, how money launderers might use the licensee's products, and the licensee's own procedures for recognizing and escalating potential money laundering;
- Audit staff — training on regulatory change, ML/TF/FP methods, and enforcement trends and their impact on the organization;
- AML/CFT/CPF compliance staff — specialized training to remain current on new trends and regulatory changes, including attendance at relevant conferences or presentations;
- Supervisors and managers — a higher level of instruction covering all aspects of ML/TF/FP policies, procedures, and regulations, reflecting their responsibility to supervise staff; and
- Senior management and the Governing Body — regular, thorough communication of ML/TF/FP issues and risks, to maintain awareness of the reputational risk such matters pose to the licensee.

Training must be given to directors, officers, employees, and relevant contractors on appointment, and refresher training must be given at least annually (Gaming Regulations, Regulation 21.8, as supplemented by this Code of Practice) and whenever needed to ensure staff remain informed of current and emerging ML/TF/FP techniques, methods, and trends. To demonstrate compliance with these training obligations, a licensee must maintain records including the content of training programs, the names of staff trained, the dates training was provided, the results of any assessment of staff understanding, and an ongoing training plan. A working template training log is provided at Annex 6.

VI.5 An Independent Audit Function to Test the Program

The compliance program must be monitored and evaluated at least annually, or more frequently where justified by the licensee's risk profile or directed by the Commission (Gaming Regulations,

Regulation 21.8), by an adequately resourced internal audit function or an outside independent party, performed by persons not involved with the licensee's AML/CFT/CPF compliance staff and sufficiently qualified to ensure their findings are reliable. The scope and frequency of testing must be commensurate with the ML/TF/FP risks posed by the licensee's products, services, delivery channels and customers. At minimum, testing must include:

- an evaluation of the licensee's AML/CFT/CPF manuals;
- review of customer files;
- review of compliance management;
- performance of transaction testing;
- assessment of training adequacy;
- assessment of compliance with applicable laws and regulations;
- evaluation of the licensee's ability to identify unusual activity;
- interviews with employees handling transactions and their supervisors;
- a sampling of unusual transactions at and beyond the applicable threshold, followed by review of compliance with internal and external reporting requirements; and
- an assessment of the adequacy of the record-retention system.

The audit should also consider whether the Governing Body was responsive to earlier audit findings. The scope and results of testing must be documented, with deficiencies reported to senior management or the Governing Body and to the MLRO, together with a request for prompt corrective action by a specified deadline, which may include enhancement of controls and procedures.

VI.6 Examination by the Commission

All licensees must provide information or documentation regarding their ML/TF/FP policies and deterrence and detection procedures to examiners of the Commission or the Regulatory Support Provider in preparation for, or during, an examination, and upon request during the year. Licensees must make the following readily available:

- their written and approved AML/CFT/CPF compliance program;
- records of their Business Risk Assessment;
- the name and job description of the MLRO and of the designated senior manager responsible for the licensee's overall ML/TF/FP policies and procedures;
- the MLRO's annual reports to the Governing Body and the Governing Body's responses;
- records of reported unusual transactions;
- records of unusual transactions requiring closer investigation;
- records of frozen accounts;
- the schedule of training provided to personnel regarding ML/TF/FP;
- the assessment report on the licensee's policies and procedures by internal audit or an external auditor; and
- customer files, including customer risk assessment, CDD, customer acceptance, and transaction information.

The Commission may assign supervisory functions under this Code of Practice to a Regulatory Support Provider (Gaming Regulations, Regulation 23), and a licensee must cooperate with the Regulatory

Support Provider to the same extent as with the Commission. Licensees must also submit such periodic and event-driven AML/CFT/CPF returns and certifications as the Commission prescribes (Gaming Regulations, Regulation 25.1).

PART VII

Supervision, Directions and Enforcement

VII.1 Directions by the Commission

The Commission may direct a licensee to adopt additional measures to handle its ML/TF/FP risk more effectively. Without limiting this power, the Commission may, in the public interest, direct a licensee not to enter into a business relationship with a specified person or class of persons, not to undertake transactions of a specified description with a specified person or class of persons, to terminate an existing business relationship with a specified person or class of persons, or to cease operations in a particular jurisdiction.

VII.2 Supervisory and Enforcement Measures

The Commission will apply supervisory and enforcement measures that are proportionate to the seriousness, duration, frequency, and consequences of the non-compliance, and to the risk presented to the integrity of gaming under the Commission's jurisdiction. The purpose of enforcement is to secure timely compliance, protect customers and the regulated sector, deter recurrence, and preserve confidence in the Commission's licensing framework.

This Part operates together with the enforcement provisions of the Gaming Regulations. Serious or repeated breach of AML/CFT/CPF, sanctions, customer due diligence or financial-crime prevention requirements may constitute serious non-compliance (Regulation 37.1(e)). The Commission may also use corrective measures and administrative monetary penalties (Regulations 38 and 39), suspension and revocation (Regulations 40 and 41), and any final decision will be communicated in writing with its reasons and any right of reconsideration, review or appeal (Regulation 42).

VII.2.1 Supervisory and Remedial Measures

Where the Commission identifies a deficiency, weakness, or emerging risk, it may require one or more of the following measures, whether or not formal disciplinary proceedings are commenced:

- a written warning, supervisory finding, or compliance direction;
- a written remediation plan with specified actions, responsible persons, milestones, and completion dates;
- enhanced reporting, independent testing, or periodic certification of compliance;
- the appointment, at the licensee's expense where authorized, of an independent auditor, skilled person, monitor, or other qualified reviewer;
- restrictions on products, payment methods, customer categories, jurisdictions, outsourcing arrangements, or other activities presenting heightened risk;
- additional License conditions, governance requirements, capital or operational safeguards, or enhanced approval requirements; and
- such other proportionate measures as are reasonably necessary to correct the deficiency or control the identified risk.

VII.2.2 Disciplinary Measures

Where non-compliance is material, repeated, deliberate, reckless, inadequately remediated, or otherwise demonstrates that a licensee or associated person may no longer satisfy the Commission's standards of suitability, the Commission may exercise any disciplinary power available under the Gaming Regulations, including, as applicable:

- a formal reprimand or public censure;
- a monetary or administrative penalty where authorized by law;
- variation, limitation, suspension, or revocation of a License, approval, registration or authorization;
- removal, disqualification, or restriction of a Key Person or other person requiring Commission approval;
- a direction to cease specified conduct, terminate specified relationships, or suspend specified transactions or operations; and
- referral of suspected criminal, sanctions, tax, fraud, corruption, or other unlawful conduct to a competent authority.

VII.2.3 Factors Considered by the Commission

In determining the appropriate supervisory or disciplinary response, the Commission may consider all relevant circumstances, including:

- the nature, seriousness, duration, frequency, and impact of the breach;
- whether the breach was deliberate, reckless, negligent, systemic, or isolated;
- the level of financial-crime or sanctions risk created by the breach;
- the adequacy of governance, staffing, systems, controls, and senior-management oversight;
- whether the licensee identified and self-reported the matter promptly;
- the quality and timeliness of remediation and cooperation with the Commission;
- any actual or potential financial benefit obtained from the breach;
- the licensee's previous compliance and disciplinary history; and
- the need for the Commission's response to be effective, proportionate, and dissuasive.

VII.2.4 Urgent Protective Action

Where the Commission reasonably considers that immediate action is necessary to protect the integrity of gaming, preserve assets or evidence, prevent continuing non-compliance, or address a material ML/TF/FP or sanctions risk, it may take any interim or emergency measure authorized by the Gaming Regulations or the terms of the License. Such action may be taken without prejudice to any subsequent investigation or disciplinary proceeding and remains subject to any procedural rights required by applicable law.

VII.2.5 Publication and Regulatory Notice

Subject to applicable law, confidentiality obligations, and procedural fairness, the Commission may publish final enforcement outcomes or regulatory notices where publication is considered necessary to promote transparency, deterrence, industry learning, or confidence in the regulatory framework. The Commission may withhold or redact information where disclosure would prejudice an investigation, expose confidential information, or create an undue risk to persons or proceedings.

VII.3 Cooperation with Foreign Regulators and Law Enforcement

The Commission may share information concerning a licensee's compliance with this regulatory instrument with foreign regulatory or law-enforcement authorities on the basis set out in Part I.6 and I.7, and may take into account reliable information received from such authorities when exercising its supervisory, licensing, or enforcement functions, subject to applicable confidentiality and information-sharing requirements.

PART VIII

General Provisions

VIII.1 Relationship to Other Instruments

This regulatory instrument must be read together with the Gaming Regulations, applicable License conditions, any standards, notices, guidance or directions issued by the Commission, and any AML/CFT/CPF, criminal, sanctions, proceeds-of-crime, privacy, or other legislation that applies by operation of law. If a conflict arises, primary legislation prevails over this regulatory instrument, and this regulatory instrument prevails over any other Commission guidance unless the Commission expressly states otherwise within the limits of its lawful authority. The Gaming Regulations apply alongside this regulatory instrument. If a conflict arises between them, the Gaming Regulations prevail, except that this regulatory instrument may impose requirements that are stricter than, and consistent with, the Gaming Regulations.

VIII.2 Transitional Provisions

This Code of Practice is effective from 1st December 2026 and is applicable to all licensees. There is no transition period.

VIII.3 Amendment

This Code of Practice may be amended at any time by resolution of the Commission. Material amendments shall be notified to licensees with reasonable advance notice, and, where practicable, following consultation with affected licensees and industry stakeholders. Each amendment shall be published together with the date on which it takes effect (Gaming Regulations, Regulation 46.5).

ANNEX 1

Definitions

Term	Meaning
AML/CFT/CPF	Anti-Money Laundering, Countering the Financing of Terrorism, and Countering the Financing of Proliferation.
Applicable Sanctions Law	Any statute, regulation, order, designation, prohibition, asset-freezing measure, or other sanctions instrument that has binding legal effect in relation to the Territory, a licensee, a person, property, or a transaction, including where applicable the Canadian federal sanctions framework referred to in Part II.5.
Beneficial Owner	The natural person(s) who ultimately own(s) or control(s) a customer, or on whose behalf a transaction is conducted, including a person exercising ultimate effective control over a legal person or arrangement.
Business Relationship	A relationship between a licensee and a customer that is expected to have an element of duration, such as the opening of a gaming account.
CDD Threshold	EUR 3,000, or the equivalent in another currency, applied to a single financial transaction or to linked financial transactions (Part IV.1), as set by this Code of Practice (Gaming Regulations, Regulation 21.11).
Commission	The Niisitapi Gaming Commission.
Compliance Officer	The individual appointed under the Gaming Regulations (Regulation 13) to oversee the licensee's overall compliance with those Regulations, applicable law, and License conditions. The Compliance Officer must be a different individual from the MLRO.
Customer Acceptance Policy (CAP)	A licensee's documented policy describing the categories of higher-risk customer, applicable risk indicators, corresponding levels of CDD, and the circumstances in which service will be declined.
Customer Due Diligence (CDD)	The measures a licensee applies to identify and verify a customer and beneficial owner, understand the purpose of the relationship, and conduct ongoing monitoring, as set out in Part IV.
Domestic Territory	Has the meaning in the Gaming Regulations: the sovereign territory of Niisitapi, within which regulated gaming services may not be offered to persons physically present (Regulation 4.1).
Regulatory Support Provider	Has the same meaning as in the Gaming Regulations (Regulation 23).
FATF	The Financial Action Task Force, an intergovernmental body established in 1989 and mandated by its member jurisdictions to develop and promote policies protecting the global financial system against money laundering, terrorist financing, and proliferation financing.
FATF Recommendations	The framework of recommendations issued by the FATF setting the international standard for combating money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction.

Term	Meaning
Financing of Proliferation (FP)	The provision of funds or financial services for the manufacture, acquisition, development, or use of nuclear, chemical, or biological weapons and their means of delivery, as further described in Part II.4.
Financing of Terrorism (FT)	The financing of terrorist acts, terrorists, or terrorist organizations, as further described in Part II.3.
Gaming Regulations	The Online Gaming Regulations.
Governing Body	The board of directors or equivalent body with ultimate management and oversight responsibility for a licensee.
Licensee / Reporting Entity	Any B2C Licensee (a B2C Operator) and, to the extent specified by the Commission, any B2B Supplier.
MLRO	The Money Laundering Reporting Officer appointed under Part VI.3 and Regulation 21.4 of the Gaming Regulations.
Money Laundering (ML)	The process by which the proceeds of criminal activity are disguised to appear to originate from a legitimate source, as further described in Part II.2.
Niisitapi Sovereign Bank (NSB)	The Niisitapi Sovereign Bank (NSB) is the statutory central bank for indigenous peoples under the Aapaitsitapii Siksikaitsitapiskahkoo Government (SASG), and acts as the financial intelligence unit (FIU) that receives reports under this Code of Practice.
Occasional Transaction	A transaction with a customer who, at that point, is not expected to return and for whom no account has been opened.
Politically Exposed Person (PEP)	An individual who holds, or has held, a prominent public function domestically or in a foreign country or international organization, together with their immediate family members and close associates, as further described in Part IV.6.
Source of Funds	The origin of the funds involved in a specific transaction, such as employment income, pension release, property or share sale proceeds, gambling winnings, gifts, or legal settlements.
Source of Wealth	The origin of a person's total accumulated net worth, such as employment, inheritance, investment, or business ownership.
Territory	The lands and jurisdiction over which the Niisitapi Gaming Commission exercises regulatory authority.
Unusual or Suspicious Transaction	A transaction or attempted transaction meeting one or more of the criteria set out in Part V.1 of this Code of Practice.

ANNEX 2

Template: List of Restricted and High-Risk Jurisdictions

This template is intended to assist licensees in documenting their own jurisdiction-risk assessment under Part III.2.3(b). The Commission may issue and update a reference list; licensees remain responsible for maintaining their own assessment.

Category 1 — Prohibited Jurisdictions

Jurisdictions in which the licensee is prohibited from offering services, whether by operation of law, sanctions, or Commission direction. This list should include at minimum the Domestic Territory (Gaming Regulations, Regulation 4.1), Canada and the US.

Category 2 — High-Risk Jurisdictions (Enhanced Due Diligence Required)

Jurisdictions identified by FATF's list of High-Risk Jurisdictions subject to a Call for Action, FATF's list of Jurisdictions under Increased Monitoring, or equivalent regional or national sources. List to be reviewed at least quarterly.

Category 3 — Jurisdictions Subject to Monitoring

Jurisdictions warranting closer monitoring based on corruption-perception indices, national risk assessments, or other credible sources, without triggering an automatic prohibition.

ANNEX 3

Template: AML/CFT/CPF Program Table of Contents

Licensees may use the following structure as a starting point when preparing the written AML/CFT/CPF Program required under Part VI:

1. Policy Statement and Senior Management Commitment
2. Governance and Approval (Governing Body / Senior Management sign-off, review cycle)
3. Business Risk Assessment (methodology, outcome, risk appetite)
4. Customer Acceptance Policy
5. Customer Due Diligence Procedures (standard, simplified, enhanced)
6. Politically Exposed Persons Procedures
7. Sanctions Screening Procedures
8. Ongoing Monitoring Procedures
9. Unusual/Suspicious Transaction Recognition, Escalation and Reporting Procedures
10. Record-Keeping Procedures
11. MLRO and Senior Manager — Roles, Authority and Reporting Lines
12. Employee Screening Procedures
13. Training Plan and Records
14. Independent Audit Plan
15. Outsourcing / Reliance on Third Parties and Group Arrangements
16. Technology and New Product Risk Assessment Procedure
17. Annexes (forms, templates, escalation flowcharts, contact list)

ANNEX 4

Template: Unusual/Suspicious Transaction Report (Internal)

For internal escalation to the MLRO under Part V.1. This is a starting template; the MLRO's external report to the Niisitapi Sovereign Bank should follow that authority's own prescribed format (for example, a goAML-style portal submission).

Field	Details
Report reference number	
Date/time of report	
Reporting employee	
Customer name / account ID	
Date(s) of transaction(s)	
Transaction amount(s) and currency	
Payment method(s)	
Indicator(s) triggered (objective / subjective)	
Description of unusual activity	
Customer risk rating at time of transaction	
Supporting documents attached	
MLRO review notes	
Decision: escalate externally / monitor / close	
Date reported to Niisitapi Sovereign Bank, if applicable	

ANNEX 5

Template: MLRO Job Description

Item	Detail
Position	Money Laundering Reporting Officer (MLRO)
Reports to	[Governing Body / Senior Management]
Independence	This position must be independent from, and must not report to, any individual with operational responsibility for gaming operations, sales, or marketing. The MLRO must not be a director of the licensee, must be a different individual from the Compliance Officer appointed under the Gaming Regulations, and has direct access to the Governing Body.

Core responsibilities

- Design, implement, and maintain the licensee's AML/CFT/CPF Compliance Program.
- Serve as the primary point of contact with the Commission and the Niisitapi Sovereign Bank on AML/CFT/CPF matters.
- Review and approve escalated unusual/suspicious transaction reports and determine whether external reporting is required.
- Maintain the Business Risk Assessment and Customer Acceptance Policy in current form.
- Design and deliver (or oversee delivery of) role-based staff training.
- Maintain all records required under Part V.6 and Part VI.4.
- Coordinate the independent audit of the Program required under Part VI.5, and track remediation of any findings.
- Report to the Governing Body at least annually, and escalate material issues without waiting, on material risks, the effectiveness of controls, significant incidents, suspicious-activity reporting, training, remediation and the current enterprise-wide risk assessment (Part VI.3).

Acceptance

I confirm that I have read and accept the above responsibilities.

Name	Signature	Date

ANNEX 6

Template: Staff Training Record

Employee Name / Role	Training Topic	Date Delivered	Trainer	Assessment Result

Ongoing training plan for the next 12 months
