NIISITAPI
GAMING COMMISSION

Know Your Customer (KYC) Policy

Document control

Item	Entry
Issued by	Niisitapi Gaming Commission
Applies to	B2C Licensees, including holders of a Provisional License
Legal basis	Regulations 18.1(a), 21 and 46 of the Online Gaming Regulations
Version	1.0 (draft)
Effective date	To be confirmed by the Commission
Policy owner	Niisitapi Gaming Commission
Review cycle	At least every two years, and after any significant regulatory change
Enquiries	Refer to the Niisitapi Gaming Commission website

Contents

Document control 1
1 Introduction and purpose 3
2 Scope and regulatory context 3
3 Responsibilities and procedures 3
4 Registration and initial verification 4
5 Screening and risk assessment 4
6 Enhanced checks and ongoing monitoring 5
7 Incomplete verification and withdrawals 5
8 Records and data protection 6
9 Reporting, training and review 6

1 Introduction and purpose

1.1 This Know Your Customer Policy is issued by the Niisitapi Gaming Commission (the Commission) to establish clear, proportionate requirements for Player identification, verification, customer due diligence and ongoing monitoring. It is the KYC Policy referred to in Regulation 18.1(a) of the Online Gaming Regulations (the "Regulations").

1.2 Licensees must achieve reliable verification while avoiding unnecessary documents, repetitive requests and unjustified delays. The extent of checks must reflect the risks of the Player, transactions, products, payment methods and markets.

2 Scope and regulatory context

2.1 This Policy applies to B2C Licensees, including holders of a Provisional License, when registering and servicing Players. A B2B Licensee carrying out checks for a B2C Licensee must support compliance with the applicable requirements; responsibility remains with the B2C Licensee. This Policy does not prescribe player onboarding for B2B suppliers that have no Player relationship.

2.2 This Policy is to be adopted under Regulation 46 of the Online Gaming Regulations and supports Regulations 18.1(a), 19.7, 19.8, 19.13 and 21. It must be read with the AML Policy, Responsible Gaming Policy, Player Complaints Policy, ADR Policy, Incident Report Policy and, where applicable, the Commission's policy on Virtual Assets (Regulation 21.1).

2.3 Terms defined in the Regulations have the same meaning here. CDD means customer due diligence; EDD means enhanced due diligence; PEP means politically exposed person; MLRO means money laundering reporting officer. Source of funds concerns the origin of money used for gambling; source of wealth concerns how the Player acquired their overall wealth.

2.4 The Regulations prevail over this Policy. Mandatory applicable law prevails as provided by Regulation 47. Any stricter applicable legal or AML Policy requirement must be met; the proportionate approach in this Policy does not waive it.

3 Responsibilities and procedures

3.1 Senior management must approve the Licensee's KYC procedures and appoint a person responsible for implementation. This may be the Compliance Officer or MLRO where suitable. The MLRO is responsible for financial crime escalation and reporting under the AML Policy.

3.2 Procedures must identify the checks used, responsible staff, escalation routes, review triggers and arrangements for incomplete verification. They may form part of the AML procedures; a separate manual or duplicate records are not required.

3.3 Where an operations manual is maintained, a short summary and reference to the current KYC procedures is sufficient. Supporting evidence must be held securely and made available to the Commission on request. Outsourcing checks does not transfer the Licensee's accountability.

4 Registration and initial verification

4.1 At registration the Licensee must obtain the Player's full name, date of birth, residential address, country of residence and contact details.

4.2 Verification must follow the timing in the AML Policy (Parts IV.1 and IV.3):

(a) at registration, and in any case before the first deposit, the Licensee must screen the Player for PEP status and sanctions (section 5) and, before the first deposit, confirm that the Player is at least eighteen (18) years old, or any higher applicable minimum age (Regulation 18.1(b));

(b) once the Player's single or linked transactions reach the CDD Threshold of EUR 3,000, the Licensee must verify the Player's identity and residential address and complete the other CDD measures in the AML Policy;

(c) in every case, the Player's identity must be verified against a valid government-issued identity document before the first withdrawal; and

(d) CDD must also be applied, whatever the amount, where money laundering or terrorist financing is suspected or the Licensee doubts identification data previously obtained.

4.3 Reliable independent electronic sources, recognised digital identity services or suitable identity documents may be used. A successful electronic check can satisfy identity, age and address verification where it reliably covers those elements. Separate uploads are not required merely because verification was electronic.

4.4 Where electronic checks do not establish identity, a valid government issued passport, identity card or driving licence may be used, supported by proportionate authenticity and ownership checks. A selfie, liveness check or certified copy is required only where justified by risk or doubts about authenticity or ownership.

4.5 The residential address must be verified through a reliable independent source. If this cannot be done electronically, an appropriate bank statement, utility bill, government correspondence or equivalent reliable evidence may be accepted. Evidence should normally be dated within six months, unless its continuing reliability is established. A utility bill is not the only acceptable evidence.

4.6 The Licensee must consider reasonable alternative evidence where standard documents are unavailable. It must record the method, result and reason for acceptance or refusal. Self-declaration alone is insufficient to verify age or identity.

5 Screening and risk assessment

5.1 Before activating an account for deposits or gambling, the Licensee must screen for applicable targeted financial sanctions and PEP status. Sources must cover sanctions binding on the Licensee and any additional lists prescribed by the Commission. Screening may be performed through a suitable service provider.

5.2 Potential matches must be checked using available identifiers. A name match alone is not a confirmed match. Confirmed sanctions cases must be handled under applicable freezing, prohibition and reporting requirements. The Player must not be permitted to transact contrary to those requirements.

5.3 PEP status is not itself a reason for refusal. Where PEP requirements apply under the AML Policy or applicable law, the Licensee must obtain senior management approval, take reasonable measures to establish source of wealth and source of funds, and apply enhanced monitoring.

6 Enhanced checks and ongoing monitoring

6.1 EDD is required where financial crime risk is high, there is a relevant PEP exposure, higher risk jurisdiction exposure, suspected false identity, unexplained third party payments, unusual transaction patterns or other material concerns. Using more than one payment method or using Virtual Assets does not, by itself, determine the risk rating.

6.2 The Licensee must identify the concern and obtain information sufficient to resolve it. Measures may include further identity evidence, payment ownership checks, an explanation of activity, source of funds or source of wealth evidence, and closer monitoring. Higher risk relationships require senior management approval in accordance with the AML Policy.

6.3 Routine source of funds or source of wealth documents are not required for every Player. Where needed, requests must be proportionate to the activity and concern. Relevant extracts and reasonable redaction of unrelated information should be accepted where they preserve the evidence needed.

6.4 Activity must be monitored for material changes, inconsistent behaviour, rapid deposits and withdrawals with little play, payment misuse, linked accounts and attempts to evade controls. Licensees must set documented, risk-based review triggers, including appropriate value and cumulative activity triggers across linked accounts under their control. No threshold permits suspicious activity to be ignored.

6.5 Verification must be refreshed where information is materially outdated, unreliable or inconsistent, or a new risk requires it. A document expiring after valid verification does not automatically require the Player to upload it again. Reasonable evidence of payment method ownership or wallet control may be sought where necessary; full card security codes, passwords and wallet private keys must never be requested.

7 Incomplete verification and withdrawals

7.1 If initial checks cannot be completed within the period set by the AML Policy, the account must not continue accepting deposits or gambling where the same unresolved concern makes those activities inappropriate.

7.2 Checks should be carried out when the need becomes apparent. A withdrawal request must not be used as the first opportunity to request information that the Licensee could reasonably have obtained earlier. New checks at withdrawal are permitted where new risk, fraud concerns, sanctions or legal obligations justify them.

7.3 The Licensee must give a clear, consolidated request stating what is needed, acceptable alternatives and how to provide it securely, unless disclosure is prohibited. Further requests must address a genuine gap or new concern. Already verified information must not be requested again without a documented reason.

7.4 KYC must not be used to avoid paying legitimate winnings, impose unreasonable conditions or encourage further gambling. An unresolved check does not, by itself, establish fraud or entitle the Licensee to confiscate balances or void winnings. Funds must remain safeguarded under Regulation 19.

7.5 A restriction must be documented, limited to what is necessary and reviewed promptly as evidence arrives. Unaffected funds must be released where lawful and practicable. Withdrawals must be completed within five working days after required checks are completed, subject to the documented exceptional circumstances permitted by Regulation 19.7. The Licensee must not prolong checks to circumvent that requirement.

7.6 If verification cannot reasonably be completed, the Compliance Officer or MLRO must decide and record the lawful next step, including continued restriction, closure, return of funds where permitted, or reporting. Suspected underage use must be blocked immediately and handled under the Responsible Gaming Policy. Funds must not be paid to a prohibited recipient or returned in breach of freezing or reporting obligations.

8 Records and data protection

8.1 Keep the information collected, verification sources and results, risk rating and reasons, screening outcomes, material requests, decisions, transaction records and relevant internal and external reports. Provider reference numbers and retrievable audit trails may be used without unnecessary duplicate storage, provided the underlying evidence remains accessible.

8.2 Retain relationship CDD records for at least five years after the relationship ends and transaction records for at least five years after the transaction, or longer where required by law or directed by the Commission, in accordance with Regulation 21.10. Records subject to a lawful preservation requirement must not be deleted. Apply a documented deletion schedule when retention obligations expire.

8.3 Collect only information needed for a legitimate purpose. Explain its use in the privacy notice, restrict access, use secure collection and storage, and control service provider access and transfers. Biometrics and sensitive documents require appropriate safeguards. Material breaches must be reported under the Incident Report Policy.

9 Reporting, training and review

9.1 Staff must promptly escalate suspicious activity to the MLRO, who must assess and report to the competent authority where required by applicable law and the AML Policy. A report to the Commission does not substitute for a legally required suspicious transaction report. Tipping off prohibitions must be respected.

9.2 Relevant staff must receive role-appropriate training on verification, fraudulent evidence, financial crime indicators, data protection and fair treatment of Players. KYC controls may be assessed within the annual independent AML review required by Regulation 21.8; a duplicate KYC audit is not required.

9.3 The Licensee must review its procedures at least annually and after a material change or control failure. Records must be available to the Commission on request. This Policy takes effect on the date confirmed by the Commission; enquiries should be submitted through its designated regulatory channel.