Sovereignty SRL
-
Customer Due Diligence Procedure

Version Control

Prepared By	Reviewed/Approved By	Revision Number	Approval Date
Sovereignty SRL	Manager	1	07/05/2025

Table of Contents

1.0 Introduction

1.1 Purpose

This Customer Due Diligence ("CDD") Procedure, otherwise known as Know Your Customer ("KYC") Procedure describes the operational procedures which must be adhered to in the execution of customer onboarding and ongoing monitoring activities, which will be carried out by the Company.

This Procedure should be read in conjunction with the Anti-Money Laundering ("AML") Policy, alongside other key compliance documentation, in addition to relevant regulation and legislation.

This Procedure follows a Risk Based Approach ("RBA") to CDD checks, which will be commensurate to the Financial Crime ("FC") risk associated to each Customer. The extent of CDD measures employed during the CDD process will be determined using the RBA, considering any red flags and mitigating factors, in order to come to a proportionate risk assessment.

1.2 Application

This Procedure must be applied to all Customers of the Company, including all players and where relevant, Third Parties ("TPs"). CDD measures must be implemented at the commencement of the business relationship (Customer Onboarding) and throughout the duration of the Customer relationship, on an ongoing basis.

1.3 Scope

This Procedure applies to all Staff and personnel of the Company.

2.0 Legal and Regulatory Basis

This CDD Procedure has been drafted in line with the relevant regulatory and legislative requirements and is aligned to the Tobique Gaming Commissions ("TGC") approach to FC, including Money Laundering ("ML") and Terrorist Financing ("TF") prevention.

2.1 Consequences of Non-Compliance

In circumstances where compliance with this Procedure is not possible, a formal Procedure waiver must obtain (see Appendix I).

3.0 Customer Onboarding Procedure

The following section has been drafted based on onboarding a natural person. For nuances where a legal entity/TP is concerned, see section 3.9.

3.1 Initiation of Customer Onboarding

CDD must be undertaken at account opening and must be completed within 30 days of the first deposit or before the Customer wagers more than an equivalent of EUR 2,000 of their own funds (as opposed to recycled winning) and before any money is paid out.

3.2 Onboarding Execution Procedure

The onboarding process is split into several phases. The initial stage is carried out at the point of registration with the following data points obtained:

Stage 1-Registration

- Full legal name.
- Email.
- Date of Birth ("DoB")

Players under the age of 18 are not allowed to register. The DoB will be input by the player, which will be checked against the current date to ensure that no underage player is allowed to register.

An email will be sent to the email address provided by the Customer at the point of registration. The email text will include a link for the Customer to follow to activate the account. This process will validate the email address provided by the Customer. If the link is not clicked, the account will not be activated and cannot be used.

At this stage it will be possible to validate (to a certain extent) the data input during the registration process. New registrations will be reviewed for odd combinations of required fields and missing or falsified personal details, with names of all Customers screened against relevant databases.

The system will also cross-check the email address provided in order to prevent duplicate or possible duplicate accounts and to prevent players from registering with duplicate email addresses.

Customers not registered are will not be allowed to deposit and place bets.

Stage 2-Completion of CDD

Full player CDD will be carried out when the thresholds identified in this procedure have been reached. These are summarized below:

- Single or cumulative deposits and withdrawals of EUR 2,000 or equivalent.
- Within 30 days of the first deposit.
- Registration details do not match with the IP location identified.
- Suspicion that a customer has multiple accounts.
- Suspicious deposit and/or withdrawal patterns; and/or,
- The deposit bank account jurisdiction differs to the withdrawing bank account jurisdiction.

Once a, or multiple thresholds have been met, complete CDD will be initiated. The Customer will be sent an email requesting a copy of:

- Valid proof of identity.
- Valid proof of residential address; and,
- Source of funds/payment verification[1].

The documents received are cross-checked with the information submitted by the Customer during the registration process. If there is any doubt about the authenticity of the documentation and the Customer is new, the Customer may be asked to provide additional documentation or a certified copy of the documentation submitted.

3.3 Customer Risk Methodology

Customers will be risk rated based on their FC risk. The following risk factors will be assessed:

- Customer Risk.
- Geographical Risk.
- Product Risk; and,
- Payment Risk.

[1] See the appendices for acceptable sources of verification

Based on the outcome of the risk assessment, the Customer will be risk rated as follows:

Risk Level	Risk Assessment Outcome	Due Diligence Level	Periodic Review Date
Lower	No red flags identified. No adverse media, PEPs or sanctions identified.	Standard Due Diligence	3 years
Standard	Medium risk red flag e.g. medium risk adverse media. No PEPs or sanctions nexus identified.		2 years
Higher	High risk red flags e.g. high risk adverse media, PEP and/or sanctions hit	Enhanced Due Diligence	1 year

3.3.1 Standard Due Diligence

Standard Due Diligence ("SDD") refers to situations where the Company will obtain minimum information on the Customer. Where SDD is applicable, Section 3.2 will be executed in full.

3.3.2 Enhanced Due Diligence

Enhanced Due Diligence ("EDD") will be executed upon the identification of the following[2]:

- A connection to a Politically Exposed Person ("PEP");
- A person connected to a sporting event.
- High risk red flag e.g. the Customer resides in a high risk jurisdiction; and/or,
- The conclusion of a High-risk Customer profile.

EDD measures implored will include:

- Additional information to verify the Customer's identity; and,
- Additional information as to the Customer's SOF.

For all Customer relationships where EDD is applied, approval will be obtained by the Nominated Compliance Officer.

[2] Note: This is not an exhaustive list and may be updated at any time. Where any doubt is identified, escalate to the Nominated Compliance Officer for guidance. All correspondence must be recorded and saved to the CDD file.

3.4 Screening

Screening will be conducted on all Customers (and Third Parties) at the point of registration and on an ongoing basis. All Customer names will be screened against relevant adverse media, PEP and sanctions lists with the following data points entered as a minimum:

- Forename.
- Surname; and,
- Year of birth.

3.5 Further Information Requests

Where further information is required, the Customer support team will email the Customer clearly detailing what additional information is needed (and where appropriate) provide an explanation for the request.

3.6 Escalation Process

For all High-risk Customers, the relationship must be signed off by the Nominated Compliance Officer. The Nominated Compliance Officer will review the Customer risk assessment and approve or terminate the onboarding/client relationship.

Reasoning for the decision made by the Nominated Compliance Officer will be clearly documented and attached to the CDD file.

3.7 Quality Check

Commensurate with the size of the Company, a sample check on CDD files will be conducted. The sample size chosen is at the discretion of the Company but will be proportionate and made on a risk-based approach. The sample check at a minimum will be conducted quarterly with the results reviewed by the Nominated Compliance Officer.

3.8 Third Party Onboarding

Where the Customer is a TP/Legal Entity, the following information must be obtained:

<u>Identification</u>

- Proof of incorporation/registration, including evidence of:

- Full legal name.
- Applicable trading/brand names.
- Registered address.
- Registered number.

- Proof of Directors,
- Proof of ownership, up to and including the identification of applicable Ultimate Beneficial Owners ("UBOs").

Verification

For the purposes of verification[3] the following must be obtained:

Risk Level	Verification Requirements	Due Diligence Level	Verification Required
Lower	X2 Directors All UBOs (up to 25%)	Standard Due Diligence	Certified Proof of Identity Proof of Residential Address
Standard			
Higher	All Directors All UBOs (up to 10%)	Enhanced Due Diligence	

4.0 Record Keeping

The Company will:

- Maintain, for at least 5 years, all necessary records on transactions, including domestic and international.
- Maintain records of the originator/payer information, and required beneficiary/payee information, on wire transfers, electronic fund transfers and other electronic payments; and,
- Keep records obtained through CDD including copies and records of official documentation account files and business correspondence, for at least 5 years after the business relationship has ended, or after the date of the occasional transaction.

5.0 Ongoing Monitoring

5.1 Periodic Review

[3] See Appendix V for the certification requirements

The Company must conduct Periodic Reviews of all Customers. The Periodic Reviews will be commensurate with the FC risk and associated risk rating of the Customer, as defined above.

Periodic Review must comprise of a full CDD refresh, including CRA, KYC information and documentation gathered in support of the CDD requirements, in addition to relevant screening checks.

5.2 Event Driven Reviews

Event Driven Reviews ("EDRs") will be comprised of a full CDD refresh, in line with that collated as part of a Periodic Review (see section above).

5.3 Transaction Monitoring

All transactions will be monitored to prevent and detect possible instances of ML or TF. Special attention will be given to complex or unusual trends and/or transactions.

Daily reports will be received and reviewed by the compliance team, who will investigate Customers transactional activity against their expected transactional profile.

Where suspicious activity is identified, the compliance team will escalate to the Nominated Compliance Officer for review and where necessary a SAR will be filed to the TGC and/or relevant FIU.

All transaction monitoring thresholds will be regularly tested and reviewed, with required changes made as soon as possible.

6.0 Off-boarding Procedure

Off-boarding of a customer may be carried out when:

- A risk is identified which is outside of the Company's risk appetite; and/or,
- The Customer requests termination of the business relationship.

The reason for closure of the account must be noted on the CDD file, with the Customer notified in writing of the period in which the off-boarding will be complete.

7.0 Suspicious Activity Reporting

<u>When to File a Suspicious Activity Report</u>

The Company must file a Suspicious Activity Report ("SAR") in the following instances:

- The reporting entity suspects on reasonable grounds that a Customer is not the person the customer claims to be;
- The reporting entity suspects on reasonable grounds that the provision, or prospective provision, of its services is related to a financing of terrorism offence, or a money laundering offence, or other criminal offence; and/or,
- A transaction, for whatever reason, does not appear to have a lawful economic purpose.

SAR Template

SAR Template	
To	Nominated Compliance Officer
Date of Report	
Prepared By	
Name of Natural Person/Legal Entity Suspected	
Name of Customer (if different to the above)	
Reason for Suspicion	
Date Suspicion First Detected	
Additional Commentary	

SAR Escalation

Where a SAR is required, it must be logged and escalated to the Nominated Compliance Officer for review. At the Nominated Compliance Officer's discretion, the SAR, (where appropriate) must be reported to the Tobique Gaming Commission ("TGC") and/or the Financial Intelligence Unit ("FIU").

Appendices

[See below examples of appendices that may be included. Please remove as applicable].

Appendix I- Compliance Waiver Template

Compliance Waiver- Email Template	
Addressed To	[Nominated Officer]

Compliance Waiver- Email Template	
Application Date of Waiver	[Date]
Reason for Waiver	[Insert Commentary]
Waiver Raised By	[Insert Individual Name]
Waiver Approved/Denied	[Y/N]
Nominated Officer Commentary	[Insert Commentary]

Appendix II- Acceptable Sources- Proof of Identity

ID Type	Acceptable Validility
Passport	As per the expiry dated on the ID
Driver's License	
National Identity Card	

Appendix III- Acceptable Sources- Proof of Residential Address

Proof of Residential Address	Acceptable Validility
Bank Statement	Dated within the last 3 months
Driver's License	As per the expiry dated on the ID
National Identity Card	
Utility Bill (electricity, gas, water etc)	Dated within the last 3 months
Mortgage Statement	Dated within the last 3 months

Appendix IV- Acceptable Sources- Source of Funds/Proof of Player Funds

Acceptable Player Source of Funds
Bank Statement
Registered debit/credit card

Appendix V- Certification Requirements

Certification is the process by which an attestation is sought regarding the authenticity of a document.

In all cases, the certification can only be provided by an independent and appropriate person as defined below:

- Legal professional.
- Notary.
- Barrister.
- Accountant; and/or,
- Consulate, embassy or high commission employee of the country of issue (acting in their official capacity.