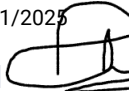


Effective Date: 01/07/2025
 Last Reviewed: 18/08/2024
 Next Review Date: 01/07/2026

07/11/2025
 Approved  

Morganite Corporate Services
 B.V. Managing Director

Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) Compliance Program

INTRODUCTION	2
GOVERNANCE AND OVERSIGHT	2
ROLE OF THE MANAGING DIRECTOR	2
APPOINTMENT OF THE COMPLIANCE OFFICER	3
RESPONSIBILITIES OF THE COMPLIANCE FUNCTION	3
CUSTOMER DUE DILIGENCE	3
PURPOSE AND OBJECTIVES	3
SCOPE	4
CDD MEASURES	4
<i>Customer Identification and Customer Verification</i>	5
<i>Identification and Verification of Legal Entities</i>	8
<i>Politically Exposed Persons (PEPs)</i>	10
<i>Obtaining information on the purpose and intended nature</i>	12
<i>On-Going Monitoring</i>	12
CUSTOMER ACCEPTANCE CRITERIA AND CUSTOMER RISK ASSESSMENT	15
CUSTOMER-RELATED RISK	15
TRANSACTION PATTERNS	17
PRODUCT, SERVICE AND TRANSACTION RISK	20
SOURCES OF FUNDS	20
GEOGRAPHIC RISK	22
DISTRIBUTION CHANNELS RISK	24
SIMPLIFIED DUE DILIGENCE	24
ENHANCED DUE DILIGENCE	25
REPORTING PROCEDURE	28
RECORD KEEPING PROCEDURE	32
EMPLOYEE TRAINING, EMPLOYEE SCREENING POLICY	33

Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Program (hereafter “the AML Program” or “AML/CFT” or “Program”) has been developed by Verse Corp B.V., a licensed gaming operator in Curaçao, in accordance with the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Landsverordening, N.G. 2017, no. 92) and related implementing decrees.

The Program is further aligned with binding regulatory guidance issued by the Curaçao Gaming Authority (CGA) as the competent supervisory body under the Ordinance, as well as with international best practices including the FATF 40 Recommendations, and is developed and implemented based on the risk-based approach (RBA), in line with Recommendation 1 of the FATF and Article 4 of the National Ordinance. The Company allocates resources proportionally to the level of identified ML/TF risk and applies enhanced measures where risks are higher and simplified measures where risks are demonstrably low.

This document sets out the internal policies, procedures, and operational controls that Verse Corp B.V. maintains to prevent its operations from being misused for money laundering, terrorist financing, or proliferation financing.

The AML Program:

- applies to all business activities involving customer onboarding, payments, account management, and gaming activity;
- is binding on all employees, contractors, and relevant third parties engaged with Verse Corp B.V.;
- is reviewed at least annually and updated as necessary to reflect changes in regulation, business model, or risk environment.

The Program has been formally approved by the Managing Director of Verse Corp B.V. and shall be effective in accordance with the date set forth above.

Governance and Oversight

Role of the Managing Director

The Managing Director of Verse Corp B.V. holds overall responsibility for the approval and effective implementation of this AML Program. The Managing Director:

- ensures that the AML Program complies with the requirements of the CGA and applicable laws;
- receives regular reports from the Compliance Officer regarding AML/CFT risks, controls, training, and reporting;

- ensures the independence, authority, and resources of the AML compliance function;
- fosters a culture of integrity, transparency, and compliance across all business units.

Appointment of the Compliance Officer

Verse Corp B.V. appoints a qualified AML/CFT Compliance Officer with sufficient experience, authority, and independence. The Compliance Officer:

- reports directly to the Managing Director;
- is not involved in commercial decision-making or operations;
- is empowered to oversee the development, implementation, and ongoing maintenance of the AML/CFT framework.

The Compliance Officer has unrestricted access to relevant records, personnel, systems, and management when performing compliance duties.

Responsibilities of the Compliance Function

The AML/CFT Compliance function is responsible for:

- maintaining and updating the AML/CFT policies and procedures;
- coordinating Customer Due Diligence and Enhanced Due Diligence processes;
- performing internal reviews of flagged accounts and escalations;
- preparing and submitting Suspicious Activity Reports (SARs) to the FIU Curacao;
- overseeing training;
- staying current with regulatory developments, risk trends, and typologies.

Customer Due Diligence

Purpose and Objectives

The purpose of this section is to ensure that Verse Corp B.V. applies robust, risk-sensitive Customer Due Diligence (hereafter “CDD”) measures in full compliance with the requirements of the CGA, in its capacity as the designated supervisory authority under Article 2(2) of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92).

This section is also aligned with the international AML/CFT standards set by the FATF, particularly Recommendations 10–12 concerning customer identification, verification, and enhanced due diligence.

The objectives of this framework are to:

- prevent the misuse of Verse Corp B.V.'s services for money laundering, terrorist financing, or financing of proliferation;
- apply risk-based identification and verification processes for all customers;
- maintain an ongoing monitoring process proportionate to the identified risk;
- escalate enhanced due diligence for high-risk customers;
- detect and report suspicious transactions to the Financial Intelligence Unit (FIU) Curacao as required under Article 25 and 26 of the Ordinance.

Scope

This CDD framework applies to all business relationships and occasional transactions conducted through Verse Corp B.V.'s gaming platforms, including registration, deposits, wagers, withdrawals, and any other financial activities.

It also applies to all employees, contractors, and third-party providers (e.g. PSPs, KYC vendors, affiliate marketers) whose roles or services may impact the AML/CFT exposure of Verse Corp B.V.

All such parties must fully adhere to the CDD measures outlined herein. Failure to do so may result in internal disciplinary action and notification to the CGA pursuant to Article 27 of the Ordinance.

CDD measures

Verse Corp B.V. has established and implemented a comprehensive set of CDD measures, in accordance with Article 7 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Landsverordening, N.G. 2017, no. 92) and in line with Recommendation 10 of the FATF.

These measures are designed to verify the identity of customers, assess their AML/CFT risk level, and ensure that all transactions conducted via the platform are consistent with the declared purpose of the business relationship.

The CDD measures applied by the Company include the following core components:

- Customer Identification and Customer Verification
- Identification and verification of Legal Entities
- Collection of Information on the Purpose and Intended Nature of the Business Relationship
- On-Going Monitoring

Customer Identification and Customer Verification

Customer Identification

Customer Identification refers to the collection of personal data and other identifying information required to uniquely establish the identity of a customer prior to the establishment of a business relationship, as mandated under Article 7(1) of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92).

The objective of this process is to ensure that Verse Corp B.V. is able to determine with reasonable certainty who the customer is, thereby reducing the risk of misuse of the platform for money laundering, terrorist financing, or related financial crimes, and to comply with regulatory expectations of the CGA.

The Customer Identification process is conducted before any gaming or financial activity is permitted. In the case of users accessing free or demo products that are functionally connected to paid services, identification shall also be performed at the initial access stage.

The minimum required information includes:

- i. full name;
- ii. date of birth;
- iii. permanent residential address;
- iv. place of birth;
- v. nationality;
- vi. identity number (where applicable)

In low-risk scenarios, determined in accordance with the Customer Risk Assessment (hereafter “CRA”) methodology outlined in this AML Program, Verse Corp B.V. may limit customer identification to a reduced set of data (typically items (i) to (iii) above), provided that the customer does not engage in activity exceeding predefined transaction thresholds and there are no risk indicators or red flags.

In high-risk scenarios (as defined in the high-risk indicators table), Verse Corp B.V. will collect a more extensive set of identifying information, which includes but is not necessarily limited to items (i) to (vi) above, and may request additional information as necessary to adequately assess the customer’s identity and risk profile.

The verification stage follows the initial identification process.

Customer Verification

Customer Verification is the process of validating that the identity information collected during the identification stage is accurate, authentic, and relates to a real and existing person, as required under Article 7(2) of the National Ordinance and consistent with FATF Recommendation 10.

Customer Verification must be completed prior to establishing a business relationship unless risk-based procedures justify a temporary deferral, in accordance with internal controls.

The verification process consists of the following core procedures:

- Document Verification
- Identity Confirmation.

Document Verification is a process of validating the authenticity and validity of the identification documents provided by the customer.

Identity Confirmation is a process of ensuring that the identity information matches the person presenting the documents.

Types of government-issued photo ID documents that can be provided by the customer:

- i. driver's license;
- ii. identification card;
- iii. passport or travel document.

These documents must be valid (not expired), contain a clear photograph, and be issued by a recognized public authority. During review, security features (e.g., holograms, watermarks, microtext) are assessed to confirm authenticity.

For verification of residential address proof any of the following documents not older than 6 months old could be obtained:

- i. bank statement;
- ii. utility bill (only fixed-line telephone bills are accepted);
- iii. official correspondence from a central or local government authority, department or agency;
- iv. rental or lease agreement;
- v. verified communication via telephone, postal mail, or email

All submitted documents should be authentic, clear, legible and of good quality.

Other verification methods that could be used are:

- i. checking social media;
- ii. telephone directories;

- iii. companies registries or media and news sources;
- iv. geo-location information;
- v. IP address data;
- vi. funding method data;
- vii. technological measures and controls e.g. biometric checks.

Informal sources such as social media or news content may only be used to support verification in higher-risk cases or to assist in resolving inconsistencies, and are not considered primary verification tools.

In certain situations, Verse Corp B.V. may request additional verification from a customer even after initial identification and verification have been completed, particularly when:

- a refund, withdrawal, or chargeback is requested;
- unusual transaction patterns or access behavior are detected;
- there are inconsistencies in account usage or login credentials.

The Company may require the customer to:

- confirm ownership of the registered email or phone number via a one-time code sent to the respective channel;
- log in and complete an authentication step through the platform interface;
- submit supplemental documentation (e.g., updated photo ID or source of funds) as needed based on the risk profile.

These additional checks are part of the Company's ongoing due diligence obligations under Articles 10 and 11 of the National Ordinance (N.G. 2017, no. 92) and serve to protect both the Company and the customer from identity fraud, unauthorized access, and abuse of the platform.

If Verse Corp B.V. is unable to obtain sufficient certainty regarding the identity of a customer, additional measures may be taken, such as:

- requesting further identification documents;
- asking for a photo of the customer holding their ID;
- requiring the first transaction to originate from an account in a reputable jurisdiction;
- sending a verification code to a validated phone number and requiring the customer to enter it.

The following behaviors or transactional patterns may be considered unusual or inconsistent with the customer's declared risk profile, and may warrant additional verification measures by the compliance function:

- multiple low-value deposits made in rapid succession or unusual patterns sudden increases in transaction frequency or volume;
- use of payment methods not associated with the verified identity or country;

- accessing the platform from multiple IP addresses or jurisdictions within a short time frame;
- use of anonymizing technologies such as VPNs;
- high gameplay velocity immediately after account registration.

Such activity does not in itself constitute suspicious behavior but may indicate the need for enhanced due diligence, temporary account restrictions, or escalation to senior compliance officers in line with the Company's Risk-Based Approach.

Once sufficient information is verified and documented, the customer is assigned an initial risk rating based on the validated data in line with the risk-based framework.

Identification and Verification of Legal Entities

While the procedures described in Section III.1 apply to individual (natural person) customers, Verse Corp B.V. may also establish business relationships with legal entities such as corporations, partnerships, foundations, or other legal arrangements. In such cases, the Company must conduct specific identification and verification procedures to confirm the existence, structure, and legitimacy of the legal entity, in accordance with Articles 7 and 8 of the National Ordinance (N.G. 2017, no. 92) and FATF Recommendation 10(c).

The following minimum information must be obtained:

- i. full legal name of the entity
- ii. type of legal form (e.g., corporation, trust, foundation)
- iii. country of incorporation or registration
- iv. registered office address and principal place of business
- v. registration or company number
- vi. names and roles of senior management or directors

The Company shall verify this information by requesting relevant documentation, which may include:

- i. Certificate of incorporation
- ii. Extract from the official business registry
- iii. Memorandum and Articles of Association (or equivalent)
- iv. Shareholder register (where applicable)
- v. Proof of business address (e.g., lease agreement or utility bill)

The nature and intended purpose of the business relationship must also be collected and assessed. Verse Corp B.V. may request:

- i. description of the business activity
- ii. expected transaction volume and counterparties
- iii. source of funds (SoF)

iv. identity and authority of individuals acting on behalf of the entity

Where risk indicators are identified — such as complex ownership, or links to high-risk jurisdictions — the Company shall apply enhanced due diligence.

The Company shall also proceed to identify and verify the Ultimate Beneficial Owner(s) (UBOs) of the legal entity, as set out in Section III.2.2.

Ultimate Beneficial Owner (UBO) Identification and Verification

In accordance with Article 8 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Landsverordening, N.G. 2017, no. 92), Verse Corp B.V. must identify the UBO(s) of a legal entity customer and take reasonable measures to verify their identity.

A UBO is defined as the natural person(s) who ultimately owns or exercises control over the legal entity, or on whose behalf a transaction or activity is being conducted. This includes individuals who:

- directly or indirectly own or control a significant interest in the legal entity (commonly interpreted, in line with international standards, as 25% or more of shares or voting rights); or
- exercise effective control through other means, such as special voting rights, control agreements, or management influence.

The 25% ownership threshold is applied as a reference benchmark in accordance with international standards (e.g., FATF), but is not prescribed by the National Ordinance. Verse Corp B.V. applies a risk-based approach and reasonable measures as required under Article 8.

If no natural person can be identified under these criteria, or if there is reason to doubt who holds ultimate control, the Company shall identify and verify the identity of the senior managing official (e.g., CEO, managing director) as the UBO, in accordance with the fallback rule recognized under the FATF framework.

The following information must be collected for each identified UBO:

- full name
- date of birth
- nationality
- residential address
- nature and extent of the ownership or control

Acceptable means of verification include:

- shareholder registers or ownership charts

- corporate registration records and official extracts
- notarized declarations of ownership
- trust deeds or partnership agreements (where applicable)
- public databases or certified third-party sources

In cases involving complex corporate structures, offshore entities, or legal arrangements designed to obscure ownership, Verse Corp B.V. will apply enhanced due diligence and may require:

- legal opinions or attestations by qualified professionals
- documentation from regulated intermediaries
- independent validation through corporate intelligence tools

The Company must ensure that no business relationship is established or maintained where the UBO cannot be identified or verified to a reasonable extent, as required under Article 10 of the National Ordinance.

Politically Exposed Persons (PEPs)

To ensure compliance with international and local sanctions regimes and mitigate risks associated with politically exposed persons (PEPs), Verse Corp B.V. conducts mandatory screening of all customers, UBOs, and authorized representatives prior to establishing or continuing a business relationship.

This process is designed to prevent the Company from engaging in transactions or relationships with:

- individuals or entities subject to targeted sanctions (financial or otherwise);
- individuals who hold or have held prominent public functions (PEPs);
- family members or known close associates of PEPs.

Sanctions Screening

Verse Corp B.V. manually screens all relevant parties against the following official sanctions lists:

- UN Consolidated Sanctions List
- EU Sanctions Map

Screening is conducted at onboarding and periodically throughout the business relationship. Any positive match must be escalated to the Compliance Officer and may result in rejection or termination of the relationship, depending on risk and legal obligations.

PEP Screening

To identify PEPs, Verse Corp B.V. uses a combination of:

- public-domain tools such as internet search engines;
- open-source governance and risk reports (e.g., [Transparency International](#));
- jurisdictional risk databases (e.g., [KnowYourCountry.com](#)).

Screening includes:

- the customer;
- the UBO (if applicable);
- the director or authorized representative;
- and known close associates or immediate family members.

Risk-Based Enhanced Measures for PEPs

Verse Corp B.V. applies EDD tailored to the risk level of each identified PEP. The following factors are considered:

- the nature and seniority of the public function;
- the jurisdiction of origin;
- the volume and frequency of transactions.

For all PEPs, the Company must:

- obtain approval from the Compliance Officer prior to onboarding or continuation;
- collect a declaration of Source of Wealth (SoW) and Source of Funds (SoF);
- validate the SoF using independent and reliable sources (e.g., public registries, financial statements, press archives);
- if public sources are insufficient, the customer may be asked to submit documentation directly;
- conduct ongoing transaction monitoring with increased frequency.

Emerging PEPs

If a customer becomes a PEP after onboarding, Verse Corp B.V. must:

- complete the EDD process described above within 30 days of identification;
- reassess the business relationship and risk profile;
- escalate to the Compliance Officer for review and approval of continuation.

Failure by the customer to cooperate or provide sufficient information may result in the suspension or termination of the relationship in line with the Company's risk-based policies and applicable legal obligations.

Obtaining information on the purpose and intended nature

In addition to identity verification, Verse Corp B.V. obtains information on the purpose and intended nature of each customer's relationship with the platform, in accordance with Article 7(1)(c) of the National Ordinance (N.G. 2017, no. 92) and FATF Recommendation 10.

This includes understanding:

- why the account is being opened;
- what level of gaming or transactional activity is expected;
- the expected source and origin of funds used on the platform.

The information is used to develop a customer's initial risk profile and to establish a basis for ongoing monitoring under Article 11 of the National Ordinance. The depth of information collected depends on the customer's risk level, and may range from self-declared statements to verified documentary evidence.

On-Going Monitoring

In accordance with Article 11 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92) and FATF Recommendation 10(e), Verse Corp B.V. conducts ongoing monitoring of all business relationships and customer transactions to ensure they are consistent with the customer's risk profile, stated purpose, and known source of funds.

Verse Corp B.V. ensures that an "ongoing transaction monitoring" is conducted to detect transactions which are unusual or suspicious compared to the customer profile. To ensure a robust ongoing monitoring system in line with the Company's risk-based approach and Article 11 of the National Ordinance (N.G. 2017, no. 92), Verse Corp B.V. has implemented a three-level control framework for transaction monitoring.

The first Line of Control:

Verse Corp B.V. works solely with trusted Payment Service Providers who all have effective AML policies in place to prevent the large majority of suspicious deposits onto Verse Corp B.V. from taking place without proper execution of KYC procedures onto the potential customer.

In addition, PSPs are expected to notify Verse Corp B.V. of any anomalies or red flags identified during their own AML procedures, including suspicious deposit patterns or blocked transactions, where applicable by law or contract.

The second Line of Control:

Verse Corp B.V. makes its network aware so that any contact with the customer or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned. In particular these include:

- requests for the execution of financial transactions on the account;
- requests in relation to means of payment or services on the account.

The Company applies a structured three-layer verification approach consisting of

- i. customer onboarding checks,
- ii. dynamic transaction risk scoring, and
- iii. targeted review by support or compliance personnel based on customer interaction and risk events.

To further strengthen its risk-based approach and meet the evolving supervisory expectations of the CGA, Verse Corp B.V. applies a Continuous Transaction Scoring (CTS) model as an extension of its dynamic risk scoring framework.

This system continuously evaluates customer behavior throughout the lifecycle of the business relationship. Risk profiles are adjusted in real-time or near-real-time based on transaction patterns, behavioral deviations, and device-level anomalies. The CTS framework ensures that emerging threats are flagged proactively, even after onboarding.

Key characteristics of CTS include:

Real-time behavioral recalibration:

A customer's risk score is dynamically adjusted based on activity inconsistent with previously observed behavior or declared profile.

Trigger events may include:

- sudden increases in deposit frequency or size;
- spikes in betting velocity (e.g., rapid wagering on high-risk games);
- unusual login patterns (e.g., access from multiple jurisdictions/IPs within a short time);
- frequent failed verification attempts or KYC circumvention behavior;
- switching to higher-risk payment methods (e.g., prepaid cards or wallets).

When such events are detected:

- the system may automatically escalate the customer's risk level from low/medium to high;
- this may trigger a manual compliance review, temporary account restriction, or EDD;

- all score changes and alerts are logged and reviewed periodically by the Compliance Officer.

CTS supports early detection of anomalous activity and aligns with Articles 10–11 of the National Ordinance (N.G. 2017, no. 92) by ensuring ongoing risk monitoring beyond static CDD.

All transactions are monitored by a three-tier verification process, which incorporates dynamic risk scoring. All customer activity is subject to continuous oversight by operational staff, supervised by the Compliance Officer.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager must also be subject to due diligence. These actions are performed under the supervision of the Compliance Officer in accordance with Article 11 of the National Ordinance, which requires the continuous monitoring of customer relationships.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behavior and the transaction counterparty.

These checks will be done by an automated system, while an employee crosschecks them for additional security.

The transactions observed on customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds should be flagged as potentially atypical and escalated for internal review when they cannot be reasonably justified based on the customer's known activity, occupation, or provided documentation.

Any Verse Corp B.V.'s employee must inform the Compliance officer of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known to the customer. Such transactions may, if unresolved or unexplained, trigger the filing of a Suspicious Transaction Report (STR) to the FIU Curaçao in line with reporting obligations under the Ordinance.

The third Line of Control:

As the last line of defense against AML Verse Corp B.V. will do manual checks on all suspicious and higher risk users in order to fully prevent money laundering.

If fraud or Money Laundering is found the case shall be escalated to the FIU Curacao and/or other competent authorities, as required by the applicable anti-money laundering legislation.

If the Company is unable to comply with the required customer due diligence measures, including identification and verification of the customer or the beneficial

owner, the business relationship shall not be established or shall be terminated. In such cases, a report will be considered to the FIU Curaçao in accordance with Article 13 of the National Ordinance.

Customer Acceptance Criteria and Customer Risk Assessment

In accordance with Articles 7 and 8 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92), Verse Corp B.V. applies customer acceptance criteria (CAP) and a formalized CRA methodology based on a risk-based approach.

The Company reviews customer risk ratings and its broader risk typologies on a regular basis or upon the occurrence of material changes, such as new product launches, emerging threats, or updates to FATF or CGA risk assessments. This ensures that the risk-based approach remains current and effective.

These criteria guide the Company's decision to initiate or continue a business relationship, and determine the required level of customer due diligence.

To mitigate the risk of money laundering, terrorist financing, and other financial crimes Verse Corp B.V. applies defined customer acceptance criteria based on risk categories, which include customer-specific factors, product/service risks, geographic exposure, and delivery channels.

Customers are assessed and classified by risk levels based on the customer-related risk, product, service and transaction risk, geographic risk and distribution channel risk and categorized into risk levels (low, medium, high).

For high-risk customers, EDD is applied in accordance with Article 8 of the National Ordinance. This may include verification of SoF, SoW, senior management approval, and more frequent monitoring. The Compliance Officer must be involved in the approval of such relationships.

Customer-related risk

The assessment of the risk posed by a natural person is generally based on the customer's economic activity and/or source of wealth. A customer having a single source of regular income will pose a lesser risk of ML/TF than a customer who has multiple sources of income or irregular income streams.

The following matrix illustrates the typical criteria used to assign risk levels based on customer-specific and transactional characteristics. This framework supports the Company's risk-scoring model, which dynamically adjusts during the lifecycle of the customer relationship.

Risk Level	Basic Information	Transaction Patterns	Source of Funds	Geographical Location
Low Risk	Valid government-issued photo ID (e.g., passport, national ID, driver's license)	Consistent with known financial profile Modest, regular transactions	Transparent sources (e.g., salary, pension)	Resides in low-risk countries with strong AML regulations
Medium Risk	Valid ID but may require additional verification	Mix of regular and occasional transactions Higher-value or less predictable transactions	Non-standard or mixed sources requiring further verification	Resides in or is associated with moderate-risk countries with developing AML frameworks
High Risk	Difficult to verify or from high-risk jurisdictions	High-value or complex transactions Frequent or significant international transfers	Opaque or involving high-risk sectors or jurisdictions Funds PEPs	Resides in or is associated with high-risk countries with weak AML regulations or sanctions

Transaction Patterns

LOW RISK		
Criteria	Characteristics	Examples
Transaction Size	Small to moderate-value transactions that align with the customer's known financial profile Regular transactions within expected ranges	Routine salary deposits Regular utility bill payments
Transaction Frequency	Regular and consistent transaction frequency Transactions that match the customer's typical activity level	Monthly rent payments Consistent business transactions such as regular vendor payments
Transaction Complexity	Simple transactions with clear and straightforward financial arrangements Low complexity in transaction structures	Direct bank transfers without intermediaries Straightforward payments for goods and services
Geographical Movement	Transactions involving low-risk jurisdictions Mostly domestic transactions or transfers to well-regulated countries	Transfers from well-regulated countries with strong AML controls Domestic transactions within a stable financial environment
Source and Destination	Transactions involving low-risk sectors Clear and verifiable sources of funds	Transactions related to well-established industries (e.g., retail, education) Funds from known and legitimate sources like salary or business income

Customer Behavior	Transactions that are consistent with the customer's known behavior Transactions with a clear and legitimate purpose	Spending patterns aligned with the customer's occupation and income level Transactions that reflect typical consumer behavior
MEDIUM RISK		
Criteria	Characteristics	Examples
Transaction Size	Moderate-value transactions that may not always align with the customer's financial profile Occasional large transactions without significant justification	Moderate international wire transfers Larger-than-normal cash deposits that are still within expected ranges
Transaction Frequency	Moderate frequency of transactions Transactions that occur periodically but are not excessively frequent	Regular monthly wire transfers or deposits Periodic large transactions such as quarterly business payments
Transaction Complexity	Transactions that have a moderate level of complexity Transactions with some layered financial structures	Transactions involving several intermediaries Transfers involving different types of financial products
Geographical Movement	Transactions involving jurisdictions with developing AML frameworks Cross-border transactions that are occasional or not highly complex	Transfers to or from moderate-risk countries Occasional international transactions involving less risky jurisdictions
Source and Destination	Transactions involving sectors with moderate risk Sources of funds that are somewhat unconventional but not highly suspicious	Transactions with moderate-risk industries (e.g., real estate) Funds from sources that are unusual but not entirely opaque
Customer Behavior	Transactions that are somewhat inconsistent with the customer's usual behavior Transactions that might have an	Slight deviations from normal spending or transaction patterns Transactions with minor discrepancies in the customer's stated source of income or business

	unclear but not overtly suspicious purpose	
HIGH RISK		
Criteria	Characteristics	Examples
Transaction Size	Large-value transactions that are inconsistent with the customer's known financial profile Frequent large cash deposits or withdrawals	Large international wire transfers Significant cash transactions without clear business justification
Transaction Frequency	High frequency of transactions in a short period Rapid movement of funds between multiple accounts	Frequent small transactions adding up to large sums Rapid transfers between accounts with no clear purpose
Transaction Complexity	Complex transaction structures involving multiple layers Transactions with intricate or opaque financial arrangements	Use of multiple accounts and intermediaries Transactions involving complex financial instruments or shell companies
Geographical Movement	Transactions involving high-risk or non-cooperative jurisdictions Frequent cross-border transactions with countries known for financial crime	Transfers to or from jurisdictions with weak AML controls Frequent cross-border transactions involving high-risk countries
Source and Destination	Transactions involving high-risk sectors or entities Unexplained or unusual sources of funds Funds from Politically Exposed Persons (PEPs)	Transactions involving high-risk industries (e.g., casinos, arms trade) Transfers from or to high-risk countries or entities
Customer Behavior	Transactions that deviate from the customer's normal behavior Transactions that lack a clear economic or legal purpose	Large one-time payments not aligned with the customer's usual transaction pattern Transactions that are inconsistent with the customer's known source of income or business activities

The assigned customer risk rating influences:

- the depth of CDD required at onboarding;
- the level and frequency of ongoing monitoring;
- the trigger thresholds for alerts and file reviews;
- the requirement to escalate for Compliance Officer approval.

Customer risk ratings are reviewed periodically or upon detection of material changes in customer behavior, business model, transaction pattern, or external risk exposure (e.g., negative media, sanctions, PEP status).

All CRA outputs must be documented, auditable, and retained in accordance with the Company's recordkeeping obligations.

Product, service and transaction risk

In accordance with Article 8(1)(b) of the National Ordinance and FATF Recommendation 10, Verse Corp B.V. assesses the inherent ML/TF risks of its products, services, and transaction types when determining the level of customer due diligence required.

Some products or services are inherently riskier than others and are therefore more attractive to criminals.

- High-risk products or services of funds typically include:
- Types of specific games (e.g. roulette, craps → even bets);
- Peer to peer gaming;
- Games involving multiple operators (poker on platforms shared by multiple operators).

At the same time, the use by customers and the acceptance by Verse Corp B.V. of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include anonymous or semi-anonymous payment channels (e.g., prepaid cards, e-wallets with limited KYC, cryptocurrencies), which must be subject to strict controls and monitoring in accordance with the Company's risk-based policy and applicable guidance from the Curaçao Gaming Authority.

Sources of Funds

Low-risk sources of funds examples:

- Salary or wages from a recognized employer
- Profits from a well-regulated business

- Regular pension payments
- Fixed rental income from property
- Bank statements showing regular deposits
- Pay stubs or employment verification letters
- Income from legitimate investments
- Earnings from legal employment or business activities
- Profits from retail or service businesses
- Payments related to education or healthcare services
- Income from countries with strong AML frameworks
- Transfers from established financial institutions in low-risk areas

Medium-risk sources of funds typically include:

- Income from businesses in emerging sectors
- Payments from international transactions involving developing countries
- Proceeds from investments in higher-risk financial products
- Income from freelance or self-employment
- Revenue from businesses with variable compliance levels
- Transfers from financial institutions in jurisdictions with moderate AML controls
- Funds from less established or new businesses

High-risk sources of funds typically include:

- Funds derived from illegal activities such as drug trafficking, human trafficking, or arms smuggling
- Income from sectors known for higher levels of money laundering or financial crime risk, such as casinos, gambling operations, or cryptocurrency trading
- Funds from PEPs. Money originating from individuals in prominent political positions, especially from countries with high corruption levels.
- Income from offshore entities with opaque ownership
- Transactions linked to entities that do not have substantial operations or legitimate business activities but serve as a cover for illicit financial flows
- Funds from high-risk jurisdictions with poor AML frameworks
- Proceeds from fraudulent schemes: Funds obtained through fraudulent activities or investment scams.
- The use by customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Multiple casino accounts or wallets.

The presence of such services does not in itself constitute a suspicion of ML/TF but necessitates a heightened level of scrutiny, especially when combined with high-risk customer behavior, payment methods, or jurisdictions.

The legitimacy and consistency of the source of funds must be assessed in the context of the customer's risk level and expected transaction behavior. In high-risk cases, supporting documentation (e.g., bank records, contracts, payslips) must be requested and reviewed before allowing continued activity.

Geographic risk

In line with Article 8(1)(c) of the National Ordinance, Verse Corp B.V. takes into account the geographic location of the customer, the source and destination of funds, and any intermediary jurisdiction involved in a transaction. Geographic risk is determined based on external assessments such as FATF blacklists/greylists, EU lists, and Transparency International's Corruption Perceptions Index.

LOW RISK		
Criteria	Characteristics	Examples
Strong AML Regulations	Robust legal framework for AML/CTF Effective enforcement of AML laws High transparency in financial reporting	Germany France Netherlands Belgium Sweden
Well-Regulated Financial Systems	Presence of competent financial regulatory authorities High standards of financial integrity Stable and well-regulated banking sector	United States Canada Australia New Zealand
Low Incidence of Financial Crime	Low levels of corruption Minimal occurrences of financial crimes Effective governance structures	Singapore Switzerland Norway Hong Kong
International Cooperation	Compliance with global AML/CTF standards Active participation in international information-sharing networks Cooperation with global regulatory bodies	EU Member States (Germany, France, Netherlands, Belgium, Sweden) North American countries (United States, Canada)
MEDIUM RISK		
Criteria	Characteristics	Examples

Regulatory Environment	Developing AML/CTF legal frameworks Variable effectiveness in enforcement Moderate transparency in financial reporting	Brazil India Mexico South Africa
Financial System Stability	Emerging or evolving regulatory bodies Financial systems in transition Banking sectors with variable standards	Turkey Indonesia Thailand Colombia
Incidence of Financial Crime	Moderate levels of corruption Presence of financial crimes but with ongoing efforts to address them Developing governance structures	Philippines Vietnam Malaysia Argentina
International Cooperation	Partial compliance with international AML/CTF standards Limited participation in international information-sharing networks Ongoing improvements in cooperation with global regulatory bodies	Kenya Egypt Bangladesh
HIGH RISK		
Criteria	Characteristics	Examples
Regulatory Environment	Weak AML/CTF legal frameworks Ineffective enforcement Low transparency in financial reporting	North Korea Iran Venezuela Syria
Financial System Stability	Poorly regulated financial sectors High levels of financial instability Lax banking sector standards	Libya Sudan Zimbabwe Afghanistan
Incidence of Financial Crime	High levels of corruption Significant occurrences of financial crimes Weak or non-existent governance structures	Haiti Central African Republic Somalia Yemen
International Cooperation	Non-compliance with international AML/CTF standards Limited or no participation in international information-sharing networks Poor cooperation with global regulatory bodies	Myanmar Turkmenistan Equatorial Guinea South Sudan

Note: The countries listed under the “High-Risk” category include jurisdictions identified by the FATF as High-Risk Jurisdictions subject to a Call for Action and/or countries under enhanced due diligence measures in accordance with international AML/CFT standards.

Distribution channels risk

The channels through which Verse Corp B.V. establishes business relationships or through which transactions are carried out may also impact the risk profile of the business relationship or transaction. In accordance with Article 8(1)(d) of the National Ordinance, Verse Corp B.V. considers the delivery channel used to initiate or maintain the relationship, especially where non-face-to-face onboarding, third-party involvement, or online-only communication is used.

Verse Corp B.V. takes all reasonable steps to eliminate anonymity and the risk associated with anonymity. These steps include requiring full verification before account activation, preventing access to gambling functions before KYC is complete, and using IP and device fingerprinting to detect proxy/VPN use.

When interacting with a customer without face-to-face basis, Verse Corp B.V. adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;

When a third party is involved in the interaction between the customer and Verse Corp B.V., there is also an increased risk. Verse Corp B.V. takes steps to ensure that there is no interaction with a third party that is not subject to any AML/CFT obligations.

Simplified Due Diligence

In accordance with Article 9 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92) and FATF Recommendation 10, Verse Corp B.V. may apply simplified due diligence (SDD) measures only where a lower risk of money laundering or terrorist financing has been clearly established, based on a documented risk assessment.

The customer verification process could be simplified but not at the detriment of AML and CTF compliance. Simplified measures must not compromise AML/CFT obligations or the Company's ability to detect and prevent misuse of its services. SDD can only be applied where there is no suspicion, and the customer does not present any high-risk indicators.

The determination of eligibility for SDD is made following an initial CRA and must be reviewed periodically.

Simplified verification is typically applied in the following scenarios:

- transactions below a certain monetary threshold, such as 4000 NAF,
- customers deemed to be low risk based on their profile, transaction history, and other risk indicators,

- situations where the customer's jurisdiction or business type is considered to have lower AML risks.

Where the CRA supports a low-risk classification and no high-risk factors are identified, Verse Corp B.V. may apply the following SDD measures, proportionate to the nature of the risk:

- not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for Verse Corp B.V. to obtain the user's identity. In this case Verse Corp B.V. may limit identification to the first three personal details (full name, permanent residential address, date of birth);
- verifying the identity of the user and the beneficial owner after the establishment of the business relationship;
- the extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, Verse Corp B.V. uses alternative reputable information sources, even where these do not contain photographic evidence of the user's identity (e.g. birth certificates, bank statements etc.);
- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD must never be applied in any of the following situations:

- Where there is a suspicion of money laundering or terrorist financing;
- Where the customer has been identified as high risk based on any factor (e.g. PEP status, jurisdiction, product usage);
- Where the customer's identity cannot be fully verified at onboarding;
- Where the transaction exceeds the applicable threshold or exhibits red flags.

Enhanced Due Diligence

In accordance with Article 8 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92), Verse Corp B.V. applies Enhanced Due Diligence where a business relationship or transaction presents a higher risk of money laundering or terrorist financing.

EDD is a mandatory requirement—not a discretionary step—where any of the following high-risk indicators are present:

- residents of higher-risk geographic areas;
- PEPs;
- products or transactions that might favor anonymity;

- new products and business practices, including new delivery mechanisms and the use of new or developing technologies for both new and existing products;
- transactions or customers associated with high-risk industries or complex ownership structures;
- adverse media reports or inconsistencies in customer-provided information;
- transactions involving high-risk jurisdictions, offshore entities, or sectors with heightened ML/TF exposure.

When such risk is identified, Verse Corp B.V. will apply the following EDD measures, which must be documented, justified, and approved by the Compliance Officer or other authorized senior management:

- obtaining additional identifying information about the customer (e.g., occupation, previous address, public source checks, press reviews, corporate registry lookups);
- collecting detailed information on the intended nature and purpose of the business relationship;
- obtaining and verifying the SoF and, where relevant, the SoW.

Acceptable examples include:

- salaries, pensions, or employment income;
- profits from legitimate businesses;
- investment earnings, dividends, share sales;
- property sales, inheritance, insurance compensation;
- gambling winnings (supported by account or payout evidence);
- obtaining information on the reasons for intended or completed transactions, particularly large or unusual ones;
- obtaining prior written approval from senior management or the Compliance Officer to establish or continue the business relationship;
- requiring the first transaction to be executed through a bank account in the customer's name at a financial institution that applies equivalent CDD standards;
- conducting enhanced and ongoing monitoring of the business relationship, with a risk-adjusted review frequency and dynamic alerting criteria.

If the customer fails or refuses to provide requested documentation during EDD without valid justification, the refusal and any related communication shall be documented and stored for compliance and audit purposes.

All EDD findings and the rationale for applied measures must be recorded in the customer file and made available for review by the Curaçao Gaming Authority or other competent bodies. Where the customer fails to cooperate or refuses to provide

sufficient information, the Company reserves the right to suspend or terminate the business relationship, in line with its risk-based approach and legal obligations.

It is recognized that unchanged customer behavior does not imply unchanged risk. Therefore, in higher-risk relationships, Verse Corp B.V. may periodically require updated Source of Funds or Source of Wealth documentation, even in the absence of observable changes in the transaction pattern or customer activity.

In accordance with Article 7(3) and Article 11 of the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92), Verse Corp B.V. shall not establish or continue a business relationship, or carry out a transaction, if it is unable to comply with the required CDD obligations.

In such cases, the Company will:

- refuse to initiate or continue the business relationship;
- reject any pending or future transactions;
- and consider whether a suspicion of money laundering (ML), terrorist financing (TF), or financing of proliferation (FP) arises, in which case a report must be submitted to the FIU Curaçao in accordance with Article 13 of the Ordinance.

Verse Corp B.V. may decide to either:

- close the account permanently, or
- lock and suspend the account in its entirety, depending on the circumstances and underlying risk.

The Company maintains detailed records of all efforts made to collect the required CDD information and documentation, including communications with the customer and internal escalation logs.

Where the customer later provides the required information or documents after an account has been blocked or terminated, the Compliance Officer shall assess:

- whether the delay in compliance increases the ML/TF/FP risk;
- whether the newly submitted documents are sufficient, reliable, and verifiable;
- whether the relationship may be reinstated or must be permanently closed based on a risk-based assessment.

Importantly, reluctance or delay alone does not automatically constitute suspicion of ML/TF/FP. Verse Corp B.V. shall evaluate the customer's behavior in context, considering:

- the reason for the delay or refusal,
- the nature and volume of past transactions,
- the customer's risk profile,

- and any red flags or inconsistencies.

If, however, a reasonable presumption of ML/TF/FP exists, Verse Corp B.V. will:

- file Unusual Transaction Report (UTR) with the Financial Intelligence Unit (FIU Curaçao) without informing the customer;
- and retain all relevant records for at least five (5) years, as required under Article 14 of the Ordinance.

Where there is no legal or regulatory reason to retain customer funds, the Company shall refund the balance to the customer using the same payment method or financial institution originally used by the customer, unless otherwise required by law or contractual obligation.

Reporting Procedure

The purpose of this procedure is to establish the process for identifying, documenting, and reporting suspicious (unusual) transactions related to potential money laundering and terrorist financing, in accordance with the requirements of the GCB and AML/CFT standards.

This procedure aims to ensure compliance with AML/CFT requirements, proper risk management associated with money laundering, safeguarding the reputation and financial stability of the Verse Corp B.V. and protecting the interests of the Verse Corp B.V. and its customers.

Compliance with this procedure is mandatory for all Employees, regardless of their position or functional responsibilities.

This procedure is especially intended for Employees who are involved in processing financial transactions, managing customer accounts and providing services to customers.

Role and Responsibility of the Compliance Officer

The Compliance Officer is responsible for analyzing and evaluating the received information about suspicious transactions.

The Compliance Officer must prepare a SAR based on the conducted assessment to report to the Financial Intelligence Unit (FIU) of Curaçao.

The Compliance officer prepares a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.

The Compliance officer keeps an adequate filing system of all records.

The Compliance Officer ensures the confidentiality of information related to the investigation and preparation of the SAR.

Employees are prohibited from disclosing information about the submission of SARs or the investigation process to unauthorized individuals.

The Compliance Officer must annually provide regulators with a report on the number and nature of suspicious transactions, as well as the measures taken to prevent money laundering.

The Compliance Officer is responsible for regularly reviewing and updating the procedure in accordance with changes in legislation and GCB requirements.

A suspicious (unusual) transaction is defined as any financial operation that does not align with the usual business activity of the customer or lacks an apparent economic or lawful purpose.

For the detection and reporting either intended or completed suspicious (unusual) transactions, Verse Corp B.V. has adequate procedures. Mentioned procedures cover:

- (a) the recognition of suspicious (unusual) transactions;
- (b) the documentation of suspicious (unusual) transactions;
- (c) the reporting of suspicious (unusual) transactions.

A suspicious (unusual) transaction is a transaction inconsistent with the player's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the player.

There are several types of indicators by which casinos must assess whether a customer's transaction qualifies as a suspicious (unusual) transaction. and that serve as the basis for filing a SAR:

- objective indicators;
- subjective indicators.

Objective indicators are specific, quantifiable signs that a transaction or activity may be linked to money laundering, terrorist financing, or other financial crimes. These indicators help to identify and assess potentially suspicious activities more effectively.

Objective indicators suggesting a suspicious (unusual) transaction:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);

c. Transactions in the amount of NAF. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.

This includes but is not limited to:

1. A cashless transaction in the amount of NAF. 5,000 or more.

A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the customer.

2. Accepting or releasing a deposit in the amount of NAF. 5,000 or more at the request of the customer;

3. Sale to a customer of chips in the amount of NAF. 5,000 or more.

"Chips" include but is not limited to tokens and credits.

4. A cash out in the amount of NAF. 5,000 or more;

A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAF. 5,000 or more and is considered per gaming day.

d. Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Subjective indicators suggesting a suspicious (unusual) transaction:

- transactions exceeding 4,000 NAF without providing convincing justification
- transactions involving unusually large amounts of cash that do not align with the customer's typical transaction patterns,
- frequent large deposits or withdrawals without apparent business justification,
- multiple transactions structured just below the reporting threshold to evade detection,
- deposits or withdrawals that appear to be intentionally designed to avoid reporting requirements,
- frequent transfers to and from countries known for high money laundering risk, or jurisdictions with insufficient AML/CFT controls,
- regular transfers between accounts without an apparent business or economic rationale,
- account activity that is inconsistent with the customer's known personal profile, such as a significant increase in volume or value of transactions,
- sudden, unexplained changes in the patterns of account use or activity,
- use of multiple accounts under the same or different names to conduct similar transactions or move funds without clear justification,
- any other operations exhibiting unusual or anomalous features.

Subjective indicators require a strong understanding of typical customer behavior and a keen sense of when something seems "off."

- unusually nervous, evasive, or secretive about their transactions or reasons for banking activities,
- inconsistent or vague explanations for the source of funds of the transaction,
- transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance,
- hesitant or refuse to provide standard documentation or information required for due diligence,
- providing information that seems to be deliberately incomplete or misleading.
- changes in an usual banking patterns without a reasonable explanation, such as sudden increases in activity or new transaction types,
- inconsistent account behavior that does not match the customer's known profile or stated business operations,
- negative media coverage or information suggesting involvement in illegal activities or associations with known criminals,
- have a history of legal issues or regulatory violations.

Documenting suspicious (unusual) transactions. Reporting of unusual transactions

For employee:

All suspicious (unusual) transactions must be reported immediately, but no later than 24 hours, to the Compliance officer in the format approved by management. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements.

For Compliance officer:

The Compliance Officer is responsible for preparing and submitting SAR.

The SAR should contain:

- identification details: Include the full name, address, date of birth, and identification numbers of the customer involved in the suspicious transaction.
- transaction details: Provide a clear description of the transaction, including the date, amount, currency, and any account numbers involved.
- reason for suspicion: Explain why the transaction is considered suspicious, detailing any red flags or anomalies compared to the customer's usual behavior.
- supporting evidence: Attach any relevant documents, such as account statements, correspondence, or other evidence that supports the suspicion.
- contact information: Provide the contact details of the Compliance officer or person responsible for submitting the report, for follow-up purposes.

Employees and management are strictly prohibited from informing any customer or third party about the filing of a SAR or the initiation of an internal AML/CFT investigation, in order to prevent tipping-off, in line with Article 13(6) of the National Ordinance and relevant FATF recommendations.

The SARs and the submission of the related information (all supporting documents) should be done in English via goAML portal at <https://portal.fiucuracao.cw>.

Reports of objective indicators to be submitted to the FIU within 48 hours of transaction taking place.

Reports of subjective indicators:

- Compliance Officer has 10 working days to complete relevant research;
- if presumption of ML/TF exists, the Compliance Officer reports within 48 hours to the FIU.
- additional information or clarification could be requested by the FIU.

Access to SARs and related documentation is restricted to authorized personnel in accordance with confidentiality principles.

The Company provides the CGA with any information, details, and reports which the CGA may consider necessary.

The reports at a minimum include reports on amendments, incidents, gambler transactions, and complaints.

All customer due diligence records, transaction data, and internal reports must be retained for at least five (5) years after the end of the business relationship or the date of the transaction, whichever is later, in accordance with Article 14 of the National Ordinance.

Record Keeping Procedure

The Record Keeping Procedure is designed to ensure compliance with AML and CFT obligations for maintaining, storing, and securing customer and transaction records.

This procedure applies to all customer identification and due diligence information, transaction records, and internal reports related to AML/CFT activities.

The types of records to be maintained include, but are not limited to:

- customer identification documents and verification data;
- transaction records including amounts, currency, and date of transactions;
- risk assessments and profiles of customers;
- records of AML/CFT-related communications;
- documentation of any internal reports filed concerning suspicious activities

Records must be accurate, complete, and up-to-date, reflecting all pertinent information necessary for verifying customer identity, assessing risk, and tracking financial transactions.

Records are maintained in integration of physical and electronic record-keeping to optimize accessibility and security, provided they are easily retrievable, secure, and protected against unauthorized access, alteration, or destruction.

Records are stored in a manner that allows for prompt retrieval by authorized personnel for the purposes of regulatory compliance, audits, and investigations.

Access to records is restricted only to personnel who require such access to perform their duties and who are authorized by the Compliance officer.

Adequate security measures, including encryption, access controls, and regular backups, are implemented to protect records from unauthorized access, tampering, loss, or destruction.

All records are treated as confidential and protected from disclosure except as required by law or regulatory authorities.

The record-keeping system is subject to periodic audits to ensure compliance with the GCB requirements and internal policies.

Upon the expiration of the retention period, records should be disposed of securely to prevent any unauthorized access to sensitive information.

Employee training, employee screening policy

This Employee training and screening policy outlines the procedures and standards established by Verse Corp B.V. to ensure compliance with the requirements. The policy is designed to ensure that all employees are adequately trained on and Countering the Financing of Terrorism regulations and that proper screening is conducted during the hiring process to maintain the integrity of our operations.

Employee training objectives are to:

- ensure all employees understand and comply with AML/CFT obligations as per GCB regulations;
- educate employees on the risks associated with money laundering and terrorist financing specific to the gaming industry;
- equip employees with the knowledge to identify, report, and manage suspicious activities effectively.

Employee screening objectives are to:

- ensure that all employees meet high standards of integrity and do not pose a risk to the Verse Corp B.V. 's compliance with AML/CFT obligations;
- comply with GCB requirements for employee screening and due diligence.

In order to recognize, prevent, and respond to risks of money laundering and terrorist financing, a structured mandatory training program is implemented and maintained. This program is tailored to the responsibilities of each employee and ensures compliance with the requirements of the Curaçao Gaming Control Board (GCB), the National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (N.G. 2017, no. 92), and international standards such as the FATF Recommendations.

Induction Training:

All new employees who will handle customers or their transactions, irrespective of their level of seniority, must undergo an AML/CFT training program as part of their induction process. This training will cover the nature and process of money laundering and terrorist financing, basic AML/CFT principles, GCB requirements, company-specific policies, explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions and the need to report any unusual transactions to the appropriate designated officer. They will also be trained on the money laundering methods and trends in the gambling sector.

Annual Refresher Training: Employees must complete refresher training annually to stay updated of current and new developments regarding money laundering and terrorist financing techniques, methods and trends, on regulatory changes, new risks, and best practices.

Role-Specific Training: Employees in high-risk roles (e.g., Compliance, Customer Service, Finance) will receive additional, targeted training relevant to their specific duties.

Training Content:

- overview of relevant laws, AML/CFT regulations, and guidelines from the GCB;
- detailed training on the Verse Corp B.V. 's AML/CFT policies, including CDD, KYC, and transaction monitoring procedures;
- training on identifying suspicious activity (recognizing red flags, transaction patterns, and customer behavior that may indicate money laundering or terrorist financing);
- training on reporting procedures (instructions on the internal reporting process for suspicious activities and compliance with SAR requirements, etc).

Training will be delivered through a combination of in-person workshops, online courses, and interactive modules.

Employees must pass an assessment at the end of each training program to demonstrate their understanding of the material.

To uphold the integrity of Verse Corp B.V.'s operations and maintain robust defenses against money laundering, terrorist financing, and other forms of financial crime, a formalized employee screening framework is in place. This framework ensures that individuals in key positions possess the requisite trustworthiness and do not present any undue risk to the company's regulatory obligations or reputation.

Screening procedures apply to all prospective employees and, where appropriate, to contractors or third parties performing sensitive functions.

Screening Process

Pre-Employment Screening

All potential employees will undergo a thorough background check before employment, including:

- identity Verification: verification of the individual's identity through official documents (e.g., passport, national ID);
- employment history verification: confirmation of previous employment, including reasons for leaving and any relevant job performance issues;
- sanctions and PEP Screening: Screening against international sanctions lists and PEP databases.

Ongoing Monitoring

Current employees in sensitive roles will be rescreened periodically to ensure ongoing compliance with Verse Corp B.V. policies and GCB requirements.

Regular audits of employee records and screening processes will be conducted to ensure that all procedures are being followed correctly and that records are up to date.

Confidentiality and Data Protection

All information obtained during the screening process will be handled confidentially and in accordance with applicable data protection laws.

Employee screening records will be securely stored and accessible only to authorized personnel.

Reporting and Compliance

Any discrepancies or concerns identified during the screening process will be reported to the Compliance Officer immediately.

Verse Corp B.V. will cooperate fully with the GCB and other regulatory bodies, providing necessary documentation and reports as required.

Review and Continuous Improvement

This Employee Training and Screening Policy will be reviewed annually to ensure its effectiveness and compliance with any new regulatory developments or operational changes.

Feedback from training sessions, audits, and regulatory reviews will be used to continually improve the policy and procedures.