



Infusion Tech B.V.

120001

Chuchubiweg 17, Willemstad, Curaçao

AML/CTF/CPF POLICY

Version 2/2025

APPROVED BY THE BOARD OF DIRECTORS

09/12/2025

Responsible Compliance Officer:

Haris Constantinou

compliance@infusiontechbv.com

Next Planned Review: December 2026

TABLE OF CONTENTS

1. Definitions	3
2. Statement of the Policy	7
3. Overview of the Online Gaming Environment	8
4. Money Laundering, Terrorism Financing & Proliferation Financing	8
5. Integration of the National Risk Assessment	13
5.1. Customer Risk Assessment	16
5.2. Ongoing Monitoring	19
6. Risk-Based Approach	21
7. Customer Due Diligence & Enhanced Due Diligence	24
8. Customer Acceptance Policy	28
9. Transaction Monitoring	53
10. Politically Exposed Persons	55
11. Sanctions Policy	56
12. Suspicious & Unusual Activity & Transaction Reporting	65
12.1. Suspicious & Unusual Activity	66
12.2. Suspicious & Unusual Transactions	67
12.3. Timely Reporting	68
12.4. Confidentiality & Commitment to the Strong Reporting Culture	68
13. Compliance Officer	68
14. Senior Management	71
15. Employee Training & Screening	72
16. AML Compliance Audit	74
17. Regulatory Access & Cooperation	76
18. Internal Audit & Reporting	77
19. Record-Keeping	79
20. Appendices	79
Appendix 1: Customer Risk Calculator	79
Appendix 2 Employee Onboarding & Screening Form	81

1. Definitions

Suspicious Activity Report/Suspicious Transaction Report – **SAR/STR**

Counter Proliferation Financing – **CPF**

A senior management member who maintains independence from the games operations, responsible for deterrence and detection of ML/TF/CPF risks – **Compliance Officer**

The Financial Intelligence Unit Curacao, referred to in art. 2 of the Norut – **FIU**

Source of Funds/Wealth – **SOF/SOW**

Know Your Business – **KYB**

The United States – **US**

Office of Foreign Assets Control – **OFAC**

Ultimate Beneficial Owner – **UBO**

Know Your Customer – **KYC**

Customer Due Diligence – **CDD**

Counter Terrorism Financing – **CTF**

Enhanced Due Diligence – **EDD**

Politically Exposed Person – **PEP**

Anti-Money Laundering – **AML**

The Caribbean Financial Action Taskforce (an organization of 24 states of the Caribbean Basin, Central and South America) – **CFATF**

Board of Directors of the Company – **BoD**

The National Ordinance on Offshore Games of Hazard (Landsverordening buitengaatsse hazardspelen, P.B. 1993, no. 63) – **NOOGH**

The European Union – **EU**

The United Nations – **UN**

Financial Action Task Force – **FATF**

The United Kingdom – **UK**

Money Laundering

The act of hiding or masking money obtained through illegal means, typically broken down into three phases: placement (introducing illicit money into the system), layering (obscuring the

money's origins through complex transactions), and integration (legitimizing the funds by reintroducing them into the economy).

AML Policy

A strategy aimed at curbing money laundering and terrorism financing, consisting of written internal policies, procedures, and safeguards. It is managed by an AML team, headed by a Money Laundering Reporting Officer (MLRO), who ensures the team receives proper training and organizes external audits of the program.

Anti-Money Laundering and Counter-Financing of Terrorism Program

A set of internal measures and controls to prevent both money laundering and terrorism financing, supervised by the AML team led by the MLRO. This person is responsible for ensuring AML-related training and auditing the program's effectiveness.

Money Laundering Reporting Officer (MLRO)

The person in charge of overseeing anti-money laundering efforts, including filing reports on suspicious transactions and enforcing AML policies and strategies within the organization.

Alert

A signal that prompts further review, triggered by certain predefined red flags or patterns, indicating potential money laundering or suspicious activity.

Beneficial Owner

The individual who has ultimate control or ownership of an account, even if it is managed by another party.

Blacklist

A list of individuals, organizations, or countries flagged for potential sanctions violations. This list is used for compliance purposes and may include internal, government, or vendor-maintained data.

Comprehensive Sanctions

Sanctions that prohibit all forms of interaction or transactions with a specific country, with very few exceptions.

Criminal Proceeds

Assets or funds that are obtained as a direct or indirect result of criminal activities.

Customer

Any individual or entity that opens an account and engages in business transactions with the Company.

Customer Relationship

All interactions between a customer and the Company from the point of onboarding through the entire lifecycle of the customer's engagement with the Company's products or services.

Know Your Customer (KYC)

A process involving the verification of a customer's identity and financial behavior, aimed at detecting unusual or suspicious activities.

Know Your Employee (KYE)

Policies to scrutinize employees to identify conflicts of interest, criminal backgrounds, or suspicious behavior that could pose risks to the company.

Due Diligence

A process of investigation and assessment of a person or entity before entering into a business relationship to ensure no legal, financial, or reputational risks are involved.

Customer Due Diligence (CDD)

Standard internal practices to confirm a customer's identity and evaluate their risk profile. It helps the company ensure compliance with regulations and mitigate risks like fraud and money laundering.

Enhanced Due Diligence (EDD)

Additional scrutiny applied to higher-risk customers, going beyond standard CDD procedures to gain a deeper understanding of their business activities and financial transactions.

High-Risk Third Country

Countries that are flagged by regulatory bodies like the European Commission or FATF due to insufficient measures to prevent money laundering or terrorism financing, thus posing significant risks.

Economic Sanctions

Measures imposed by one or more nations to influence another nation's policies, usually in the form of trade or financial restrictions.

Mandatory Sanctions Lists

Official lists required by law or regulation for organizations to check against when conducting business, such as UN Security Council Resolutions or local sanctions lists.

Egmont Group of Financial Intelligence Units

A global network of financial intelligence units (FIUs) that facilitates cooperation, training, and information-sharing to combat money laundering and terrorist financing.

Embargo

A government-imposed ban on trade or commercial activity with a specific country or product category.

European Union (EU)

A political and economic union of European countries that, among other things, sets regulations for combatting money laundering and terrorism financing across its member states.

Exclusions List

A list maintained by the compliance team containing names that have been cleared and excluded from further sanctions screening.

Financial Action Task Force (FATF)

An international organization that sets global standards for combating money laundering and terrorist financing. It also produces reports on emerging risks and trends in these areas.

Greylist

A list of countries or entities that have been identified as having weak anti-money laundering frameworks, but are working to address deficiencies.

Financial Intelligence Unit (FIU)

A national agency responsible for receiving and analyzing reports of suspicious financial transactions and forwarding them to the appropriate authorities.

First Line of Defense

The initial level of an organization's compliance framework, consisting of employees who interact directly with customers and gather relevant information to ensure proper screening.

Inherent Risk

The level of risk present before any mitigating measures or controls have been applied.

Investigation

The process of examining and gathering information in response to potential violations of sanctions or financial crimes.

Layering

A phase in the money laundering process where illicit funds are moved through various transactions to obscure their origins.

Minor

An individual under the age of 18.

Monitoring

The ongoing review of customer activity to detect unusual patterns or behavior, often aided by automated systems.

Office of Foreign Assets Control (OFAC)

A US Treasury Department agency responsible for administering and enforcing economic sanctions against foreign nations, organizations, and individuals.

Politically Exposed Person (PEP)

An individual in a prominent public position, such as a government official, whose financial transactions may require closer scrutiny due to the potential for corruption or illicit activities.

Red Flag

A warning sign indicating potential suspicious behavior or transactions that warrant further investigation.

Regulatory Agency

A governmental body responsible for overseeing financial institutions, issuing regulations, and enforcing compliance with laws.

2. Statement of the Policy

Infusion Tech B.V. has established a robust Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) Policy to address risks associated with money laundering, terrorist financing, and proliferation financing. This policy is crafted to comply with both local and international regulatory standards, providing a comprehensive framework to manage risks related to customer activities, product and service offerings, payment systems, geographical exposure, and delivery channels.

The Board of Directors (BoD) at Infusion Tech B.V. assumes full responsibility for approving, implementing, and overseeing the AML/CTF/CPF Policy. This policy undergoes an annual review to ensure alignment with evolving regulations and operational needs. Additionally, updates may be introduced promptly to address significant changes in AML/CTF/CPF frameworks or upon recommendations from internal or external AML audits, with considerations given to associated risks and operational impacts.

Infusion Tech B.V.'s policy is designed to align with the core objectives of Curaçao's AML/CTF/CPF regulatory framework, including adherence to the National Ordinance for Games of Chance (LOK), the Criminal Code of Curaçao, the National Ordinance on Offshore Games of Hazard (NOOGH), the National Ordinance Penalization of Money Laundering (NOPML), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and the National Ordinance on Identification when Rendering Services (NOIS), all reflecting the amendments effective as of May 16, 2024. The policy also ensures compliance with the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act.

To further enhance its scope, the AML/CTF/CPF Policy incorporates international best practices and guidelines, such as the Financial Action Task Force (FATF) Recommendations, the European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs), and the Wolfsberg Principles.

In summary, the AML/CTF/CPF Policy of Infusion Tech B.V. is designed to meet the expectations of Curaçao's AML/CTF/CPF supervisory authority, the Curaçao Gaming Control Board. All directors, employees, and officers of the company, along with any external consultants engaged for audits, are required to adhere strictly to the principles and guidelines detailed within this policy.

3. Overview of the Online Gaming Environment

Infusion Tech B.V., a legal entity established in Curaçao. The company is licensed under Curaçao Gaming Control Board with license number OGL/2024/1567/0779 issued 07/11/2024 . This license mandates compliance with Curaçao's regulatory requirements and imposes strict restrictions on service provision in specific jurisdictions. As such, Infusion Tech B.V. refrains from offering remote gaming services in the United States, Australia, Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. The company strictly adheres to this policy, operating exclusively in regions where online gambling is legally permitted, without targeting markets where such activities are prohibited.

The online gaming and betting sector, including entities like Infusion Tech B.V., is inherently exposed to several money laundering risks. These include identity theft, fraudulent activities, structuring of transactions, layering of illicit funds, and potential collusion between employees, customers, or external payment providers to bypass internal controls. Recognizing these challenges, Infusion Tech B.V. remains committed to implementing robust security measures to mitigate such risks effectively.

4. Money Laundering, Terrorism Financing & Proliferation Financing

Money laundering is a fundamental component of financial crimes that often extend across international borders. It supports a range of illegal activities, including tax evasion, sanctions violations, fraud, corruption, illegal arms trade, drug trafficking, extortion, and kidnapping. The primary objective of money laundering is to conceal the illicit origins of proceeds by masking their source, identity, and destination.

Key Stages of Money Laundering

1. Placement:

The initial stage involves introducing illicit funds into the financial system. Common methods include depositing funds into bank accounts, purchasing high-value goods, or conducting other financial transactions. This phase aims to start blending illegal funds into the legitimate economy.

2. Layering:

In this stage, funds are subjected to a series of complex transactions designed to obscure their origin. Techniques include transferring money across multiple accounts, converting currencies, or investing in financial instruments. The objective is to create a convoluted transaction trail that hinders efforts to trace the funds back to their source.

3. Integration:

The final stage involves reintroducing the laundered money into the legitimate economy. This is achieved by purchasing luxury assets, investing in cash-intensive businesses, or conducting other legal transactions. By this point, the funds appear legitimate, making them more challenging to link to their illicit origins.

Online gambling platforms can be vulnerable to exploitation during any of these stages. This underscores the importance of the company avoiding anonymous services and flagging suspicious activities.

Relation to Terrorist Financing

Terrorist financing involves providing financial support for terrorist activities. While these funds may originate from legitimate sources, they are often moved through financial systems using methods akin to money laundering. For instance, prepaid cards are frequently used to procure materials for terrorist operations. Staff members are trained to stay informed about emerging threats and trends in this area.

Risk Management and Compliance

To mitigate money laundering risks, Infusion Tech B.V. employs proactive strategies to identify and counter potential threats. Key measures include:

- **Verification Fraud and Identity Theft:** Conducting comprehensive customer due diligence, including verifying identity, age, and location documentation.
- **Multiple Accounts and High Transaction Volumes:** Monitoring for unusual patterns, such as the use of multiple accounts or significant transaction volumes.
- **Illicit Fund Deposits:** Detecting and addressing instances where funds from illegal activities are deposited or the platform is misused as a holding account.
- **Player-to-Player Transfers:** Preventing the platform's exploitation for transferring illicit funds or facilitating unauthorized cash-outs.

These efforts are part of a dynamic approach, with regular risk assessments to address emerging concerns. Infusion Tech B.V. also prioritizes ongoing employee training to enhance awareness and strengthen its internal Anti-Money Laundering (AML) compliance programs.

Terrorism Financing

Terrorist financing refers to the provision of financial resources, sourced through both lawful and unlawful means, to support terrorist activities. These funds are crucial for enabling operations ranging from minor incidents to large-scale attacks.

Sources of Funds

1. Legal Sources:

Terrorists may exploit legitimate avenues such as businesses, charitable donations, and other lawful transactions to funnel funds. For instance, charitable contributions or seemingly routine business dealings might be manipulated to support terrorist activities.

2. Illegal Sources:

Criminal activities serve as a significant source of financing. These include drug trafficking, fraud, smuggling, extortion, and money laundering, all aimed at obscuring the origins of illicit funds to evade detection.

Methods of Fund Transfer

Funds for terrorist activities are often moved using both formal and informal channels:

- **Formal Channels:** These include traditional banking systems and financial institutions. Tactics like layering and structuring are commonly employed to mask the source and destination of funds, minimizing the risk of exposure.
- **Informal Channels:** Non-traditional systems, such as hawala networks, operate outside regulated financial frameworks. These channels are challenging to monitor due to their decentralized nature and reliance on personal trust.

Indicators of Terrorist Financing

Detecting terrorist financing often involves identifying irregular financial behaviors. Key indicators include:

- Unusual transaction patterns that deviate from established business or personal norms.
- Frequent or large fund transfers linked to high-risk regions or known terrorist affiliates.
- Suspicious activities in high-risk industries or financial actions that appear designed to obscure terrorist operations.

Combating Terrorist Financing

To counter the risks associated with terrorist financing, Infusion Tech B.V. implements robust Anti-Money Laundering (AML) measures, including:

- **Customer Due Diligence (CDD):** Ensuring thorough verification of customer identities and financial activities.
- **Transaction Monitoring:** Actively tracking and analyzing financial activities for unusual patterns.
- **Sanctions Compliance:** Adhering to established sanctions lists to prevent transactions that might inadvertently support terrorism.

Sanctions lists observed by the company include the Sanctions National Ordinance (SNO, N.G. 2014, no. 55), the Kingdom Sanction Act (N.G. 2016, no. 54), and announcements from the Curaçao Gaming Control Board (GCB). Additionally, lists from the Office of Foreign Assets Control (OFAC), United Nations Security Council, European Union, and U.S. List of Foreign Terrorist Organizations are incorporated to ensure comprehensive compliance.

International Guidelines and Enforcement

Global efforts to combat terrorist financing are supported by:

- **Financial Action Task Force (FATF):** Setting international standards for identifying and reporting suspicious transactions related to money laundering and terrorist financing.

- Office of Foreign Assets Control (OFAC): Enforcing U.S. economic sanctions and managing the Specially Designated Nationals (SDN) list, which identifies entities involved in terrorism.
- European Union (EU): Mandating member states to implement AML measures and enforce international sanctions to prevent the financial system's misuse.
- United Nations (UN): Imposing sanctions and maintaining lists of individuals and entities linked to terrorism, contributing to global disruption of terrorist funding networks.

By adhering to these frameworks and leveraging advanced monitoring systems, Infusion Tech B.V. reinforces its commitment to identifying and preventing terrorist financing while maintaining compliance with international regulations.

Proliferation Financing

Proliferation financing refers to the financial support provided for the development, acquisition, or production of weapons of mass destruction (WMD), including nuclear, chemical, and biological weapons, as well as their delivery systems. Such financing poses significant risks to global security, and Infusion Tech B.V. is fully committed to preventing its involvement in any activities related to proliferation financing. As a licensed casino operator in Curaçao, Infusion Tech B.V. adheres to both local regulations established by the Curaçao Gaming Control Board (GCB) and international standards to mitigate risks associated with proliferation financing.

Sources of proliferation financing

1. **Legal Sources:** Proliferation financing may originate from legitimate business activities, such as trade, investments, or charitable donations, which can be exploited by proliferators to funnel money towards the development of WMDs. Infusion Tech B.V. ensures that all transactions, particularly those involving international trade or high-risk regions, are subject to thorough scrutiny to prevent misuse in the financing of WMDs.
2. **Illegal Sources:** Similar to other forms of illicit financing, proliferation financing can stem from criminal activities such as smuggling, fraud, and money laundering. Infusion Tech B.V. works diligently to identify and prevent any illicit financial activity that may be used to support proliferation-related objectives. By maintaining a robust monitoring system, the company aims to detect and disrupt illicit funding sources early in the process.

Funds used for proliferation financing may be transferred through both formal and informal financial channels:

- **Formal Channels:** Financial institutions, including banks and payment processors, are frequently used for proliferation financing. These funds may be layered through complex transactions designed to obscure their origin and destination. Infusion Tech B.V. employs advanced transaction monitoring systems to detect suspicious activities, especially when funds are routed through formal banking systems in a manner that appears designed to conceal the purpose of the transaction.

- **Informal Channels:** Informal financial systems, such as trade-based financing or alternative remittance networks, can also be exploited for proliferation financing. These systems, operating outside of regulated financial institutions, present a significant challenge to detection. Infusion Tech B.V. actively monitors for transactions that may involve high-risk jurisdictions or goods that could potentially be used in the development of WMDs, ensuring that all transactions comply with both Curaçao regulations and international sanctions.

Infusion Tech B.V. has implemented comprehensive monitoring to detect potential proliferation financing, including the following indicators:

- **Unusual Trade Transactions:** Transactions involving dual-use goods—items that can be used for both civilian and military purposes—are closely monitored. Infusion Tech B.V. identifies transactions involving countries or entities linked to proliferation activities, ensuring that trade through the platform does not inadvertently support WMD development.
- **Inconsistent Business Practices:** Infusion Tech B.V. remains alert to transactions that appear to lack legitimate business purposes or that are structured in ways designed to evade detection. Suspicious patterns, such as frequent or large transactions that are inconsistent with a customer's normal business activities, are flagged for further review.
- **Suspicious Patterns in Financing:** The company monitors transactions for signs of money laundering or the misdirection of funds intended for legitimate purposes. Transactions involving high-risk regions or known proliferators are flagged and investigated for potential involvement in WMD financing.

Infusion Tech B.V. employs a robust set of measures to combat proliferation financing:

- **Enhanced Customer Due Diligence (CDD):** Infusion Tech B.V. conducts comprehensive customer due diligence (CDD) to verify the identities of its customers, particularly those engaged in international trade or operating in high-risk industries. The company ensures that customers and transactions are legitimate, and that there are no links to proliferation financing or activities involving WMDs.
- **Transaction Monitoring:** The company uses state-of-the-art transaction monitoring systems to detect irregular patterns, particularly in high-risk transactions. Unusual or suspicious activities, such as large cross-border payments, will trigger further scrutiny to ensure that the funds are not being used for illicit purposes, including the financing of WMDs.
- **Sanctions Compliance:** Infusion Tech B.V. adheres to both local and international sanctions programs, including those enforced by the United Nations, the European Union, and the U.S. Office of Foreign Assets Control (OFAC). The company ensures that no transactions are conducted with entities or individuals listed on sanctions lists related to the development or proliferation of WMDs.

Infusion Tech B.V. follows both local Curaçao regulations and global standards aimed at preventing proliferation financing, including:

- **Curaçao Regulations:** As a licensed casino operator in Curaçao, Infusion Tech B.V. adheres to the regulations set forth by the Curaçao Gaming Control Board (GCB) and complies with the relevant national ordinances, including the National Ordinance Penalization of Money Laundering (NOPML) and the National Ordinance on the Reporting of Unusual Transactions (NORUT). These regulations require operators to implement strict anti-money laundering (AML) measures to detect and prevent illegal financing, including that related to WMD proliferation.
- **Financial Action Task Force (FATF):** Infusion Tech B.V. follows FATF recommendations, which include guidelines for identifying and preventing the misuse of financial systems for proliferation financing. By adopting FATF's recommendations, the company ensures that its compliance program is in line with international best practices.
- **United Nations (UN) and European Union (EU) Sanctions:** Infusion Tech B.V. adheres to sanctions lists and regulations issued by the UN, EU, and U.S. OFAC. These sanctions are critical in preventing financial resources from flowing into the hands of entities or individuals involved in the development of WMDs. The company carefully monitors transactions to ensure compliance with these global efforts to curb the proliferation of dangerous weapons.

Through its adherence to local Curaçao regulations and international standards, Infusion Tech B.V. ensures that its operations are free from any involvement in the financing of weapons of mass destruction. By employing rigorous monitoring systems, conducting enhanced customer due diligence, and complying with global sanctions, the company actively contributes to global efforts to prevent the spread of WMDs and enhance international security.

5. Integration of the National Risk Assessment

Infusion Tech B.V. maintains a robust and dynamic AML/CTF/CPF compliance framework designed to protect its online gaming operations, financial channels, and service infrastructure from exploitation by criminal actors involved in money laundering, terrorist financing, or proliferation financing. This framework is implemented in alignment with the legislative and regulatory framework of Curaçao, complies with the expectations of the Curaçao Gaming Control Board (GCB), and reflects international standards established by the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF). All internal and external parties including employees, senior executives, partners, and third-party providers are expected to operate within the parameters of this compliance framework.

Governance and Oversight

The Board of Directors of Infusion Tech B.V. holds ultimate responsibility for establishing, overseeing, and enhancing the company's AML/CTF/CPF compliance programme. The Board ensures adequate allocation of resources, human, financial, and technological, to effectively

manage the risks inherent to the remote gaming industry. The Senior Management team plays a key role in implementing operational measures, promoting a culture of risk awareness, and ensuring the Compliance Officer has unrestricted access to relevant systems, records, and personnel to fulfil their duties effectively.

Compliance Officer and Integration of NRA Findings

The appointed Compliance Officer is responsible for implementing and managing the day-to-day operations of the AML/CTF/CPF compliance programme. This includes conducting client due diligence (CDD and EDD), overseeing transaction monitoring, handling suspicious activity reports, managing internal investigations, and maintaining direct communication with the Financial Intelligence Unit of Curaçao (FIU-Curaçao) and other supervisory authorities. In line with AML Regulation III.1, the Compliance Officer ensures that the internal controls and operational practices of Infusion Tech B.V. are adapted to reflect national and global developments in financial crime risks.

Infusion Tech B.V. incorporates the findings of the most recent National Risk Assessment (NRA) of Curaçao into its enterprise-wide risk management approach. The Compliance Officer systematically reviews published NRA reports and evaluates their implications across the business, including the risk classification of customer profiles, product types, payment channels, operational jurisdictions, and emerging financial technologies.

Application of NRA Insights

The insights from the NRA directly inform Infusion Tech B.V. Institutional Risk Assessment and influence its risk-based approach across all AML/CTF controls. Specific actions taken in response to NRA findings may include:

- **Enhancement of identification and verification protocols** for customer onboarding;
- **Adjustment of transaction monitoring thresholds** to better capture red flags;
- **Application of enhanced scrutiny** for jurisdictions, client types, or payment methods deemed high-risk in the NRA;
- **Implementation of real-time monitoring rules** and alerts based on evolving typologies described in national reports.

As new risks or typologies are identified in NRA publications, the Compliance Officer evaluates the adequacy of the existing control environment and recommends enhancements as needed.

Risk-Based CDD and EDD Informed by NRA

Infusion Tech B.V. enforces stringent Know Your Customer (KYC) procedures before processing withdrawals or when customer activity reaches predefined thresholds based on value or behaviour. As part of its CDD procedures, the company verifies identity, age, payment method ownership, and residential address. Where risk indicators, particularly those mentioned in the NRA, are identified, enhanced due diligence (EDD) measures are applied. These may involve:

- Collection of source of funds and source of wealth documentation;
- Screening for adverse media and regulatory warnings;
- Requiring executive approval for continued engagement with the client.

EDD is routinely applied to clients in high-risk jurisdictions, politically exposed persons (PEPs), high-value or VIP clients, and those exhibiting complex or suspicious transactional patterns.

Continuous Monitoring and Reporting Protocols

The company operates a hybrid model combining automated surveillance technologies with manual review mechanisms to ensure continuous monitoring of client behaviour. The monitoring framework includes:

- Frequency and value of deposits;
- Irregular betting behaviour;
- Use of anonymisation tools or IP mismatches;
- Abuse of promotional offers or account features.

Alerts are automatically triggered for anomalous activity and are routed to the Compliance Officer for immediate investigation. All Unusual Transaction Reports (UTRs) and Suspicious Transaction Reports (STRs) are filed through the FIU Curaçao's goAML platform in accordance with AML Regulation IV.1 and the National Ordinance Reporting of Unusual Transactions (NORUT).

All employees are trained to promptly escalate red flags and are bound by strict confidentiality obligations. Any breach of confidentiality or tipping-off is considered a serious offence and may result in disciplinary or legal consequences.

Recordkeeping and Employee Training

Infusion Tech B.V. retains all compliance-related documentation, including customer due diligence files, transaction monitoring data, alerts, internal investigations, training records, and NRA-relevant assessments, for a minimum of five (5) years in line with Curaçao's AML legislation.

The company delivers mandatory AML/CTF/CPF training to all relevant staff, with special modules covering the latest NRA developments and national vulnerabilities. Training is refreshed annually and may be supplemented following regulatory updates or emerging risks. The AML/CTF framework is reviewed annually and amended where necessary to reflect NRA insights, legal changes, or new guidance issued by the GCB.

5.1. Customer Risk Assessment

Infusion Tech B.V. applies a structured risk assessment methodology to evaluate each customer's potential exposure to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). This approach relies on a client risk scoring model that assesses multiple factors, such as behavioral trends, transactional conduct, geographic exposure, and other warning indicators. The purpose of this model is to ensure a proportionate response to different levels of risk and to determine the level of due diligence and monitoring that should be applied in each case.

The scoring system assigns a specific weight to each individual risk factor, and the total score produced by this calculation determines the customer's overall risk classification. Based on the resulting risk score, the applicable level of due diligence is determined, along with the internal approvals required for onboarding and continued monitoring. The risk categories are outlined as follows:

Category	Score Range	Due Diligence Level	Approval Required
----------	-------------	---------------------	-------------------

Low Risk	0 – 1.8	Standard Due Diligence	Client Service or Compliance Officer
Medium Risk	1.8 – 2.5	Standard Due Diligence	Client Service or Compliance Officer
High Risk	2.5 or above	Enhanced Due Diligence	Approval by Compliance Officer and subject to annual review
Unacceptable	Based on qualifying risk factors	Rejected outright	Automatically rejected with no exceptions

Customers classified as low or medium risk are subjected to standard due diligence (SDD) procedures, which include identity verification and basic monitoring. However, if a customer's profile reaches the high-risk threshold, enhanced due diligence (EDD) measures are triggered. These measures involve obtaining additional documentation, senior-level approval, and periodic reassessment at least once every 12 months.

Any client identified with characteristics deemed to pose unacceptable risk, such as those flagged for links to sanctioned entities, irreconcilable inconsistencies, or clear ML/TF indicators, will be denied access to services automatically and without the possibility of escalation.

This categorization model enables Infusion Tech B.V. to effectively manage its client portfolio by aligning its risk exposure with appropriate levels of scrutiny and compliance control. The risk scoring methodology is reviewed and updated periodically to reflect evolving threats, regulatory expectations, and lessons learned from internal and external investigations.

Client Risk Scoring and Treatment

The client's risk score determines the appropriate approach to identification, information collection, and transactional oversight. Regardless of the assigned risk level, Infusion Tech B.V. ensures that every client undergoes mandatory screening for Politically Exposed Persons (PEPs), sanctions exposure, and negative media. These screenings take place both during onboarding and throughout the business relationship. For specific technical parameters, refer to **Appendix I**.

Categorization and Applied Measures Based on Risk Level

Low Risk

Clients in this group are deemed to present a minimal risk of money laundering or terrorist financing. However, due to the elevated inherent risk associated with remote gambling activities, Simplified Due Diligence (SDD) is not applied under any circumstances. Clients classified as low risk are subjected to Standard Due Diligence (SDD) procedures in accordance with the company's policies and applicable regulations.

Medium Risk

This category includes clients whose profiles exhibit moderate risk factors. While these clients do not trigger enhanced scrutiny, they require careful monitoring and standard Know Your Customer (KYC) measures. The company performs periodic reviews to ensure that all relevant information remains accurate and the risk categorization continues to reflect the client's behavior and transactional activity.

High Risk

Clients assigned a high-risk rating are subject to Enhanced Due Diligence (EDD) requirements. Prior to onboarding or continuing a relationship, Compliance Officer approval is mandatory. Individuals or entities may be classified as high risk in cases such as:

- Operating through unusual or opaque company structures.
- Conducting transactions that deviate significantly from their established profile or from typical behavior for similar client categories.
- Having connections to jurisdictions considered high-risk or under international sanctions.
- Being designated as a PEP, or being a family member or close associate of a PEP.
- Receiving a high-risk rating at the onboarding stage or during ongoing monitoring due to multiple contributing factors such as exposure in adverse media, high-frequency or high-value deposits, and irregular gambling activity.
- Presenting falsified or unverifiable identification or documentation.
- Executing transactions that appear to lack a clear economic rationale or legal justification.
- Representing entities engaged in financial intermediation, such as those holding funds on behalf of others or processing payments for clients.
- Reaching cumulative deposit amounts exceeding thresholds defined as indicative of high-risk behavior.

Unacceptable Client Profiles

Infusion Tech B.V. automatically rejects any business relationship with individuals or entities that fall into prohibited categories, including:

- Persons or organizations appearing on domestic or international financial sanctions lists.
- Individuals who are suspected of engaging in money laundering or terrorist financing activities.
- Anyone under the legal gambling age of 18.
- Clients whose sources of wealth or funds cannot be substantiated or verified through reasonable due diligence.
- Clients displaying behavioral or transactional patterns that mirror known fraudulent schemes or abuse mechanisms within the gaming industry.

The company maintains a strictly defined risk appetite, aligned with both regulatory requirements and its internal control framework. Relationships that conflict with this risk appetite are not pursued. All risk assessments and client classifications are clearly documented, supported by justifications, and subject to regular review and revision in line with evolving risk indicators and operational developments.

5.2. Ongoing Monitoring

Infusion Tech B.V. maintains a firm commitment to the continuous monitoring of customer relationships in accordance with its risk-based approach and its legal obligations under the applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulatory framework. This ongoing monitoring is designed to ensure that customer profiles remain accurate, due diligence information is consistently up to date, and that any unusual or suspicious activity is promptly identified and escalated.

Regular Screening Activities

The Compliance Department is responsible for conducting systematic and frequent screenings of customers against databases containing records of Politically Exposed Persons (PEPs), internationally recognized sanctions lists, and sources of adverse media. Where screening results in positive matches that are confirmed to be accurate, the cases are escalated accordingly and may result in the initiation of an event-driven review.

Event-Driven Reviews

Specific triggers or changes in client circumstances may necessitate a reassessment of the customer's risk profile. In some cases, this may lead to a complete refresh of the due diligence documentation on file. Event-driven reviews are initiated under the following circumstances, among others:

- When new information is obtained that undermines the accuracy, completeness, or reliability of previously collected customer due diligence (CDD) data.
- When client behavior or transaction activity raises suspicion or appears inconsistent with expected norms.

When there is a material change in the customer's risk indicators or exposure.

In such situations, Infusion Tech B.V. performs an immediate reassessment of the client's risk classification and updates all relevant records and documentation, regardless of the risk category previously assigned to the customer.

Periodic Reviews

Infusion Tech B.V. conducts scheduled periodic reviews of all customer profiles to ensure that information is accurate, reliable, and reflective of current circumstances. These reviews are based on the client's risk level and follow a predefined frequency, as outlined below:

- Clients classified as **High Risk** are subject to annual reviews. These reviews involve re-verification of residential address, re-confirmation of the source of funds and source of wealth, screening for negative news or adverse media, and a thorough evaluation of all transactional behavior and product usage during the period under review.
- Clients classified as **Medium Risk** are reviewed every two years. During these assessments, the Compliance Team confirms residential address details, verifies updated financial background information, conducts adverse media screening, and assesses the client's transactional and betting activity.
- Clients classified as **Low Risk** are reviewed every three years, unless a trigger event necessitates an earlier review. These evaluations involve address re-verification and a review for any negative news. The purpose of the review is to confirm whether the low-risk classification remains appropriate or should be updated.

Trigger events that may result in unscheduled reviews include:

- The appearance of new information that calls into question the reliability or completeness of the CDD data previously collected.
- The detection of behavioral or transactional activity that deviates from expected client patterns or profiles.
- Developments in regulatory obligations, industry risk indicators, or changes introduced by the supervisory authorities that require immediate adjustments to internal procedures.

NRA-Based Adjustments

Monitoring procedures and customer review protocols are periodically reassessed in accordance with the updates provided in the latest version of Curaçao's National Risk Assessment (NRA). Where the NRA identifies heightened vulnerabilities or introduces revised national priorities, Infusion Tech B.V. updates its internal monitoring strategies, control measures, and client evaluation models to ensure alignment with national expectations and sectoral trends. This reassessment is critical to maintaining a dynamic and responsive compliance infrastructure that accurately reflects evolving money laundering and terrorism financing risks at the national and international levels.

6. Risk-Based Approach

Infusion Tech B.V. applies a comprehensive risk-based approach to detect, manage, and mitigate potential abuse of its online gaming services for money laundering, terrorist financing, or proliferation financing. This methodology is anchored in the Financial Action Task Force (FATF) recommendations and incorporates both quantitative and qualitative evaluations of threats, vulnerabilities, mitigating controls, and potential impact across operational activities.

The company conducts a formal Business Risk Assessment (BRA) on an annual basis, as well as in response to any material modifications in the operational structure, product portfolio, or applicable legal frameworks. The risk assessment is documented, formally approved by the Board of Directors, and updated when necessary to reflect emerging threats or regulatory expectations.

Client Risk

Clients constitute a primary channel of exposure to financial crime. Infusion Tech B.V. assesses individual client risks by analyzing factors such as the complexity of the customer's financial

situation, irregularities in behavioral patterns, and connections to high-risk jurisdictions. Politically Exposed Persons (PEPs), clients with opaque or diverse sources of income, or those whose financial behavior significantly deviates from declared income are subject to increased scrutiny.

Clients classified as low risk typically maintain a clear and traceable income source and show consistent account behavior. In contrast, clients with inconsistent transactions, unidentified or complex sources of funds, or substantial volume of financial activity are flagged for enhanced due diligence and subject to more stringent monitoring measures.

Product, Service, and Transaction Risk

Some product types and transaction models present a heightened level of risk. Infusion Tech B.V. identifies elevated risks associated with the use of cryptocurrencies, digital wallets, prepaid instruments, and peer-to-peer mechanisms, particularly where these may obscure the provenance of funds.

To address these threats, the company applies tailored controls, including transaction caps, real-time surveillance, and automated detection alerts. These tools are configured to identify outliers such as large one-off bets, rapid fund turnovers, and behavioral patterns inconsistent with the client's profile.

Geographical Risk

The jurisdictional footprint of the client is another determinant of risk. Clients located in or associated with jurisdictions that have weak AML/CTF controls, high levels of corruption, or are subject to financial sanctions are considered higher risk.

Infusion Tech B.V. assesses geographic risk using authoritative public sources including the FATF, Caribbean FATF (CFATF), the European Commission, OFAC, the US State Department, and Transparency International. Where links to such high-risk regions are found, the company implements enhanced controls or restrictions, including mandatory due diligence checks and additional transaction verification requirements.

Distribution Channel Risk

The method through which a customer interacts with the platform also influences risk. Digital onboarding channels, particularly those with no in-person verification, are considered more vulnerable to identity fraud and misuse.

To mitigate distribution risk, Infusion Tech B.V. employs robust digital verification processes, including the use of biometric validation, multi-factor authentication, and document verification tools. The due diligence process is consistently enforced across all platforms to ensure full regulatory coverage.

Technological Development Risk

Before deploying new technologies or significantly altering its digital architecture, Infusion Tech B.V. performs formal and documented assessments of potential technological risks. Each assessment includes a written review of the intended functionality, risks and vulnerabilities, proposed mitigation measures, and an evaluation of residual risks.

This process applies to the launch of new gaming platforms, payment integrations, artificial intelligence tools, blockchain applications, or any other innovation that may affect financial crime risk exposure. All assessments are preserved in the company's compliance records and are available for inspection by the Curaçao Gaming Control Board when requested.

Sector-Specific Risk in Online Gaming

As a licensed operator in the online gambling industry, Infusion Tech B.V. acknowledges the heightened exposure of the sector to illicit financial flows. Techniques such as high-volume, short-duration betting patterns, bonus exploitation, or staged winnings are examples of methods criminals may use to launder funds.

To mitigate these threats, Infusion Tech B.V. restricts the use of anonymous payment tools, mandates the use of regulated financial intermediaries for all transactions, and screens accounts for suspicious behaviors such as coordinated gameplay or excessive transaction recycling.

Mitigation and Monitoring

Risks that are identified through the BRA or other channels are addressed using specific countermeasures. These include enhanced documentation requests, limits on account activities, or elevated transaction monitoring protocols. The company uses both automated tools and manual review to detect and respond to potential threats.

All clients and Payment Service Providers (PSPs) are assigned a risk rating during onboarding and reassessed at regular intervals or when red flags arise. Monitoring includes ongoing screenings for adverse media exposure, updates to sanction status, and confirmation of PEP status.

Recordkeeping and Reporting

Infusion Tech B.V. maintains comprehensive records relating to client risk classification, due diligence activities, monitoring efforts, and business risk evaluations. These documents are stored securely and preserved in line with applicable legal retention periods. Where suspicious activity is detected, timely reporting to the Financial Intelligence Unit (FIU) Curaçao is carried out, and tipping-off is strictly prohibited.

Governance and Accessibility

The company maintains structured documentation for both the Business Risk Assessment (BRA) and Customer Risk Assessment (CRA), covering inherent and residual risk analysis for products, services, jurisdictions, and client segments. These records are reviewed and updated periodically and are made accessible without delay to the Curaçao Gaming Control Board or any other authorized regulator upon request.

7. Customer Due Diligence & Enhanced Due Diligence

Before establishing any client relationship, Infusion Tech B.V. is obligated to determine whether the individual poses any potential risks related to money laundering (ML), terrorist financing (TF), or proliferation financing (PF), which could jeopardize the platform's compliance and integrity. The Client Due Diligence (CDD) process is a core component of the company's risk-based framework, aimed at detecting indicators of suspicious activity by evaluating client behavior, transaction history, profile characteristics, and how they interact with the company's services.

This process involves several essential steps, such as identifying and verifying the prospective client's identity and age, collecting supporting data to establish an economic background, calculating a risk score, and observing the client's behavior for any anomalies that may indicate breaches of anti-financial crime regulations. Publicly available data is also used for these assessments, including social media reviews, checks for property ownership, employment status, insolvency, and similar information.

Where risk levels are assessed as low, the company may consider simplified due diligence; however, enhanced due diligence is compulsory if red flags emerge such as association with politically exposed persons (PEPs) or clients residing in high-risk jurisdictions.

Infusion Tech B.V. relies on a structured client risk scoring model which assigns risk levels based on key parameters such as client geography, transaction volume, and usage of specific gambling services. To reinforce platform security, the company integrates advanced technologies and third-party compliance tools. These include anti-fraud software, artificial intelligence, biometric verification, and compliance platforms such as LexisNexis and WorldCheck.

The company's framework prohibits the use of anonymous or fictitious player accounts. A legitimate and fully verified identity is required for all players. When any anomalies or suspicious activity are detected through monitoring tools, reports are immediately submitted to the Financial Intelligence Unit (FIU) and, if necessary, to law enforcement.

Through the Client Acceptance Policy (CAP), clients are categorized into risk tiers: low, medium, or high based on factors such as jurisdiction, financial activity, and source of funds. The policy also defines conditions under which client onboarding or continued engagement must be declined due to unacceptable risk levels. Full details are provided in Appendix IV.

Application of Client Due Diligence Measures

CDD is applied under the following circumstances:

- When a transaction equals or exceeds NAF 4,000, whether executed once or in aggregate.
- When suspicion arises concerning involvement in financial crimes.
- When there is doubt regarding the validity or adequacy of previously obtained identification.
- When several smaller transactions are grouped and exceed the NAF 4,000 threshold.

In situations presenting a heightened level of risk, enhanced due diligence measures are applied without exception.

The company's CDD activities include:

- Identity verification using reliable and independent sources, including determining and validating beneficial ownership for legal entities and understanding control structures.

- Ongoing monitoring of transaction behavior to ensure consistency with the client's known risk profile, with verification of the source of funds where required.
- Ensuring that internal reporting of suspicions takes precedence over standard due diligence procedures, particularly when FIU escalation is necessary.

Identity Verification and Information Collection

To accurately verify player identity, Infusion Tech B.V. collects:

- Full name
- Residential address
- Date and place of birth
- Nationality
- Identification number

While only basic data is collected from low-risk clients, high-risk cases require a broader set of documentation to sufficiently assess ML/TF risk. Risk ratings assigned at onboarding are adjusted over time as more information becomes available.

Methods of identity verification include:

- Examination of government-issued ID documents (e.g. passport, national ID)
- Proof of address through documents such as utility bills or bank statements (dated within the past six months)
- Verification of residential details through direct contact (email, call, or physical mail)
- Use of biometric tools, verification of payment source, and IP tracking

When initial verification is inadequate, further actions such as a video selfie with ID or first deposit verification through a licensed payment provider may be initiated.

In higher-risk cases, additional information is gathered, such as details about the client's wealth origin and expected transaction volume. For medium- or low-risk customers, employment status or type of business activity may suffice, with discretionary supplementary checks.

Timing of CDD Measures

Client verification is conducted at the earliest possible stage of engagement, in full compliance with relevant AML/CTF/CPF legislation.

During registration, clients provide their full name, date of birth, and address. These details are verified as a minimum standard. Any transaction, single or cumulative, reaching the NAF 4,000 threshold triggers a full identification process. This also applies to linked transactions that together exceed this threshold within a defined timeframe.

In most instances, CDD is carried out proactively at the time of registration to minimize potential exposure.

If the verification process is not completed in time, the following restrictions apply:

- For deposits: No further deposits or withdrawals are permitted, though gameplay with existing funds is allowed.
- For withdrawals: The account is suspended pending identity verification.

If a client fails to complete CDD within 30 days:

- Suspicious activity results in an STR submission to the FIU.
- If no red flags are found, the remaining balance is returned to the original funding source.
- If risks persist, internal protocols may require account freezing.

Throughout all of the above, the company prevents “tipping off” by maintaining confidentiality and strict staff protocols.

Monitoring continues after onboarding, with regular reviews and updates to client risk ratings depending on behavioral or regulatory developments.

Specific triggers for CDD reapplication include:

- Large or irregular financial activity
- Relocation or changes in residency
- Designation as a PEP
- Changes to regulatory obligations
- Reaching NAF 4,000 in cumulative transactions again

Legacy accounts opened prior to the current regulatory standards are reviewed and updated accordingly, prioritizing those with higher-risk profiles.

Where verification is incomplete or the risk unacceptable, the relationship is terminated. The Compliance Officer reviews such cases before closure. If ML/TF/PF is suspected, an STR is immediately filed. Records are retained for at least five years after account closure.

Third-Party Reliance

In certain controlled scenarios, Infusion Tech B.V. may use qualified third parties to perform specific CDD functions. However, accountability for the due diligence process remains with Infusion Tech B.V., and all legal obligations must still be met.

The company ensures that such third parties are regulated under equivalent AML laws and contractually obligated to provide full access to records, participate in audits, and follow data-sharing protocols.

Third-party reliance is distinct from outsourcing. In reliance scenarios, the third party operates independently; in outsourcing, they function under the direct policies of Infusion Tech B.V.

Before selecting a provider, the company performs a jurisdictional risk review, evaluates the provider's track record, and conducts regular performance reviews. All decisions regarding risk classification and acceptance remain under the exclusive control of Infusion Tech B.V.

Beneficial Ownership and Control Structure Verification

Infusion Tech B.V. makes every reasonable effort to identify and validate the ultimate beneficial owners (UBOs) of corporate clients. This includes:

- Identifying individuals with direct or indirect ownership of 25% or more
- If none are identified, determining control via voting rights, board influence, or legal arrangements
- Mapping ownership structures involving trusts or layered entities
- Reviewing corporate documents such as shareholder registers and organizational charts

In cases where ownership cannot be confirmed, the most senior managing official is documented as the UBO in accordance with international practices.

All ownership data is verified with credible sources, recorded in secure systems, and updated as needed. The company will not engage with entities that obscure or obstruct the due diligence process.

8. Customer Acceptance Policy

Infusion Tech B.V. has established this Customer Acceptance Policy (“CAP”) to set out specific procedures, roles, and internal safeguards for evaluating and approving prospective clients seeking access to its licensed online gaming and betting services. The core objective of this policy is to protect the Company from being misused for unlawful activities, including but not limited to money laundering, financing of terrorism, proliferation financing, fraudulent conduct, circumvention of sanctions, or other forms of financial or regulatory crime. At the same time, the policy ensures full adherence to the applicable legal and regulatory framework governing gambling operations in Curaçao.

This CAP forms a key pillar of Infusion Tech B.V. broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance regime. It is designed in line with the supervisory requirements issued by the Curaçao Gaming Control Board and is also informed by internationally recognized standards such as those issued by the Financial Action Task Force (FATF), the AML Directives of the European Union, and the Wolfsberg Group’s financial crime compliance principles.

The Policy is underpinned by various legislative instruments in force in Curaçao, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Compliance with this policy is mandatory for all individuals involved in the client lifecycle, including directors, officers, employees, contractors, and any third parties performing onboarding tasks on the Company’s behalf. No customer may be permitted to fund their account, submit withdrawal requests, or participate in gambling or betting activity until all acceptance criteria have been satisfied and all verification, screening, and documentation procedures have been completed.

Scope of the Policy

This policy applies without exception to all natural persons and legal entities attempting to register an account with Infusion Tech B.V., regardless of the channel used for onboarding. This includes account registration via the Company’s main website, mobile applications, affiliate networks, or third-party integration platforms.

The Customer Acceptance Policy governs the full lifespan of the customer relationship, beginning from the point of initial registration and extending through all subsequent account activities until final closure or account termination. It applies to every product and service offered by Infusion Tech B.V. that falls under the Company's Curaçao gaming license OGL/2024/1567/0779.

Customer Acceptance Integration

Infusion Tech B.V. limits access to its services only to those clients who comply with all relevant legal, regulatory, and internal eligibility criteria. All applicants must confirm that they have reached the legal gambling age of at least eighteen (18) years, or any higher minimum threshold applicable in their jurisdiction of residence. Additionally, customers must provide complete, truthful, and verifiable personal data during the registration process. This includes legal name, place and date of birth, nationality, and a valid residential address.

The Company does not allow onboarding of individuals or entities based in, transacting from, or otherwise associated with jurisdictions that are either explicitly prohibited under Curaçao law, listed under international sanctions programs, or identified by the Company as high-risk or blocked for strategic or regulatory reasons. As part of the onboarding process, Infusion Tech B.V. performs sanctions screening against major global and regional watchlists, including databases maintained by the United Nations, European Union, United States Office of Foreign Assets Control (OFAC), United Kingdom's Office of Financial Sanctions Implementation (OFSI), and any applicable national lists governed by the Sanctions National Ordinance and Kingdom Sanction Act.

Clients are permitted to deposit and use only funds originating from lawful and clearly identifiable sources. Where the customer's risk profile triggers a higher degree of scrutiny, the Company reserves the right to request supporting evidence to validate the source of funds or, where necessary, the broader source of wealth. Infusion Tech B.V. also retains the right to deny access to any customer who has a documented pattern of abusive or fraudulent behavior, including chargeback fraud, bonus exploitation, or past account closures due to regulatory violations or self-exclusion related to gambling addiction.

Risk-Based Approach

Infusion Tech B.V. implements a structured Risk-Based Approach (RBA) for the onboarding and continuous assessment of its clients to ensure that customer due diligence (CDD) measures are appropriate to the specific risk each individual or entity may present. This approach enables the Company to apply differentiated controls and monitoring, based on a range of risk factors such as financial profile, transactional behavior, geographic exposure, and the use of certain access technologies.

Customer Risk Profiling

Each potential customer undergoes an evaluation to determine the likelihood that their relationship with the platform could present risks linked to money laundering, terrorist financing, or proliferation financing. Depending on the outcome of this assessment, Infusion Tech B.V. applies an appropriate level of scrutiny tailored to the identified risk.

Customers with straightforward financial circumstances such as salaried employment in low-risk sectors and gambling behavior aligned with their income level are generally categorized as low-risk. In contrast, clients may be classified as high-risk if their financial background is difficult to trace, if they work in high-exposure industries (such as virtual assets or financial intermediation), or if their gambling patterns deviate significantly from declared means. Politically Exposed Persons (PEPs), their close associates, and family members are automatically categorized as high-risk and are subject to enhanced measures.

High-risk clients are subject to Enhanced Due Diligence (EDD), which involves more rigorous identity verification, additional documentation requests, and sustained monitoring throughout the business relationship. Examples of high-risk scenarios that would prompt EDD include:

- Clients with inconsistent or unverifiable income who must present supporting documentation such as tax filings, payslips, or company financials.
- PEPs and their related persons, who require senior management approval, validated proof of source of funds and wealth, and continuous risk monitoring.
- Players whose gaming activity surpasses what would be considered reasonable based on declared financial standing.
- Unusual or unexplained changes in gaming behavior or the use of proxy accounts or intermediaries in financial transactions.
- Detection of account duplication or linkage between multiple accounts controlled by the same individual.

- Requests for large withdrawals without significant gameplay history, particularly in cases involving third-party agents or junket operators.

To maintain accuracy in customer classification, Infusion Tech B.V. continuously reviews and, where necessary, updates risk ratings in response to changes in customer behavior, large transactional shifts, or exposure to new jurisdictions. When a client's risk level increases, the Company imposes further checks such as supplementary due diligence, temporary account limitations, and higher scrutiny of transactions.

Geographic Risk Assessment

The Company conducts detailed geographic risk assessments for each customer based on their declared residency, operational location, or the source country of their funds. These assessments are updated regularly using risk data and jurisdictional insights from reputable bodies such as the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the European Commission's list of high-risk countries, the U.S. Office of Foreign Assets Control (OFAC), the U.S. State Department's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from countries under active sanctions are automatically rejected at the onboarding stage. Those from high-risk jurisdictions may only proceed if they pass EDD requirements and receive formal approval from senior compliance personnel.

High-risk countries typically demonstrate traits such as insufficient AML/CTF enforcement, widespread corruption, associations with terrorist financing networks, or active sanctions by recognized international bodies. Infusion Tech B.V. ensures its onboarding and review mechanisms are aligned with the latest publications and advisories issued by FATF, CFATF, and similar authorities. If a new or existing customer is found to be residing in or transacting from a flagged jurisdiction, the case is immediately referred to the Compliance Officer for an in-depth review and application of full EDD protocols. These include verification of identity using credible documentation, thorough analysis of the client's financial background, and intensified monitoring for the entire duration of the relationship.

Risk Assessment Workflow

The risk classification procedure integrates external risk sources and internal controls as follows:

- Upon registration, a customer's country of residence and fund origin are screened against real-time risk intelligence and global watchlists.
- Applicants from jurisdictions classified as low risk are subjected to standard CDD procedures.
- Customers from elevated-risk countries are escalated for further review and may only proceed upon completing EDD and receiving compliance clearance.
- Prospective clients from jurisdictions subject to international or domestic sanctions are immediately disqualified from account creation and a record of such rejection is maintained.
- Risk evaluations are subject to real-time updates and are automatically revised upon the availability of new risk indicators or changes to global sanctions regimes.

Product, Service, and Transaction Risks

The risk level assigned to a customer is significantly influenced by the types of products, services, and transactional behaviors they engage in. Certain features of online gaming inherently present elevated risks due to limitations in transparency and traceability. This includes services such as peer-to-peer transfers, in-platform token exchanges, or the use of payment methods with limited identity linkage such as prepaid cards or specific types of cryptocurrencies.

Accounts that display transactional behavior inconsistent with legitimate gaming usage such as large deposits followed by minimal or no gameplay activity before requesting withdrawals are treated with heightened scrutiny. Likewise, any payment instrument not registered in the customer's name automatically triggers additional verification protocols to ensure the legitimacy of both the source and the account holder.

To counter these risks, Infusion Tech B.V. has implemented a targeted monitoring system that focuses on critical transactional risk areas. It is a strict requirement that all deposited funds originate from lawful, documented, and verifiable sources. In cases where the origin of funds raises concern, for instance, potential links to criminal activity such as theft, drug trafficking, or fraud, the customer must provide credible documentation verifying the lawful source of the funds. Any transaction deemed suspicious is reported to the Financial Intelligence Unit (FIU) in accordance with applicable legislation.

Payment mechanisms that afford a degree of anonymity, including prepaid cards and certain digital assets, are classified as high-risk. These channels are subjected to strict verification

procedures, which include full documentation on the source of funds. The Company also enforces the requirement that accounts are used strictly for genuine gaming participation. Indicators of misuse such as repeated deposits and withdrawals with negligible or no betting activity, immediately trigger a risk review and may result in temporary account suspension during investigation.

When customers initiate payments using third-party financial instruments, these transactions are flagged for enhanced verification. This process involves verifying the identities of both the account holder and the third-party payee, confirming their relationship, and validating the legitimacy of the funds being transferred. Transfers between two gaming accounts are generally disallowed unless a legitimate and well-documented justification is provided. In such instances, prior approval must be obtained from the Compliance Officer, and complete records of the transaction are retained in accordance with recordkeeping requirements.

The operation of multiple accounts or wallets across any platforms operated by the Company is treated as a red flag. Infusion Tech B.V. internal surveillance systems are configured to detect and cross-reference linked accounts in order to ensure full transparency of user activity. This allows the Company to monitor for potential account splitting or concealment of betting patterns across multiple profiles. Customers who frequently alter their funding methods or banking information without clear justification may also be flagged for review, as this behavior could signal an attempt to mask the true origin of funds. These patterns prompt a comprehensive review and may result in the application of Enhanced Due Diligence (EDD) procedures.

The Company enforces a robust identity verification framework to prevent impersonation and detect identity fraud. Suspected incidents are immediately escalated to the appropriate enforcement or regulatory authorities in accordance with the applicable legal framework. Special attention is given to electronic wallet providers, particularly those licensed in jurisdictions known to have weak AML/CTF oversight or that operate under legal structures which make it difficult to trace the ownership of funds. Customers using such services must provide proof of the origin of the funds, and the Company performs checks on the licensing status and AML compliance standards of the service provider prior to approving transactions.

Channel and Technology Risk

The level of risk associated with a customer also depends on the channels and technologies used to access Infusion Tech B.V. services. Remote onboarding, while offering convenience,

introduces an increased risk of identity fraud or impersonation. To mitigate this, the company employs advanced digital Know Your Customer (KYC) solutions. These include biometric verification, document authenticity checks, geolocation validation, and multi-factor authentication.

Before deploying new technologies, payment solutions, or platform features, Infusion Tech B.V. conducts a comprehensive risk assessment. This process ensures that any innovation introduced cannot be exploited for money laundering, fraud, or other illicit purposes.

To manage channel and technology-related risks effectively, the company closely monitors several risk indicators. Any method that enables customer anonymity is treated as high risk and triggers enhanced verification procedures. These procedures may involve validating identification documents, conducting biometric checks, and performing real-time screenings against sanctions lists and Politically Exposed Person (PEP) databases.

While remote interactions are standard within the industry and not inherently risky, they still necessitate robust security measures. Infusion Tech B.V. uses secure verification technologies such as biometric authentication, liveness detection, and automated document checks to safeguard against impersonation and fraud during the onboarding process and ongoing transactions.

When third parties are involved in client interactions, the overall risk profile increases. This is particularly true when the intermediary is not subject to AML or CTF regulatory oversight. In such scenarios, Infusion Tech B.V. applies due diligence procedures to both the client and the third party. These procedures include verifying the intermediary's regulatory standing, assessing the strength of their internal compliance framework, and ensuring all submitted information is accurate and independently verifiable.

Risk Indicators

Infusion Tech B.V. utilizes a comprehensive set of predefined risk indicators to evaluate the potential level of financial crime risk each customer may pose. These indicators support the company's risk-based approach and ensure the due diligence process is appropriately aligned with the identified risk level of each individual or entity.

The risk assessment covers several core dimensions:

Customer Risk Profile – this includes aspects such as irregular or multiple sources of income, designation as a Politically Exposed Person (PEP), excessive or uncharacteristic gambling expenditures, abrupt behavioral changes, the presence of intermediaries, duplication of accounts, unexplained redemption of funds, and links to high-risk groups or junket-related operations.

Product, Service, and Transaction Risk – red flags under this category include evidence or suspicion that proceeds may be derived from criminal conduct, reliance on anonymous or loosely regulated payment instruments, inappropriate use of customer accounts, funding by unrelated third parties, regular switching of payment options, suspected identity theft or document falsification, or the simultaneous use of several digital wallets.

Geographic Risk – applies to individuals with ties to countries lacking robust AML/CFT controls, those with high indices of corruption, jurisdictions under international sanctions, or regions associated with terrorist financing. This includes territories identified by the Financial Action Task Force (FATF), the Caribbean Financial Action Task Force (CFATF), the Office of Foreign Assets Control (OFAC), or Transparency International’s Corruption Perceptions Index (CPI).

Channel and Technology Risk – includes scenarios where customers engage through channels that obscure identity, use remote onboarding without robust verification, or operate via unregulated intermediaries lacking appropriate AML/CFT controls.

To determine the overall risk category of a customer, Infusion Tech B.V. applies an internal Risk Calculator that attributes weighted values to each risk factor. The total score determines the applicable due diligence level:

Risk Level	Requirements
Low Risk	Standard Customer Due Diligence (CDD) applies, with documentation limited to what is legally required or triggered by a change in risk profile.
Medium Risk	Standard CDD plus additional verification steps and closer ongoing monitoring.

High Risk	Full Enhanced Due Diligence (EDD), senior management approval prior to onboarding, and enhanced ongoing monitoring.
------------------	---

This methodology provides consistency and objectivity in customer risk classification, allowing the company to deploy resources efficiently and in line with its regulatory responsibilities.

Risk Indicators Table

Factor	Low Risk	Medium Risk	High Risk
Purpose of Account	Recreational or casual gaming.	Professional-level gambling or consistent high-stakes play.	Bonus exploitation or behaviour aimed at financial abuse of promotions.
Source of Funds	Regular salary, savings, pensions, or other low-risk income.	Business income, legitimate casino winnings, sale of personal assets, inheritance, or documented loans/gifts from family or friends.	Unverified cryptocurrency, offshore accounts, or other unverifiable sources.
Source of Wealth	Long-term employment income, ownership of established businesses, verified inheritance, or steady investment growth.	Sale of property or business, significant lottery or gambling winnings.	High-risk investments such as cryptocurrency or forex trading, offshore holdings, or unverifiable assets.
Transaction Frequency	Occasional, typically monthly.	Regular, often weekly.	Frequent, typically daily.
Transaction Value	Up to 1,000.	Between 1,000 and	Over 4,000.

(NAF)		4,000.	
Incoming Payments	Standard bank transfers or debit/credit card deposits.	E-wallet or prepaid card deposits.	Cryptocurrency, third-party funding, deposits from high-risk jurisdictions, unusually high deposits, or use of unregulated processors.
Outgoing Payments	Normal withdrawals of winnings or deposit refunds.	Bonus-related withdrawals, frequent withdrawals, or large single withdrawals above 4,000.	Cryptocurrency withdrawals, third-party payments, chargebacks, or suspicious withdrawal patterns linked to other accounts.
Gaming Behaviour	Casual, moderate, and consistent play patterns.	Frequent high-stakes betting, extended play sessions, or fluctuating wagering amounts.	Aggressive betting patterns, rapid stake increases, loss-chasing, multiple accounts, collusion, or other fraudulent indicators.
Payment Channels	Traditional bank transfers.	Verified e-wallets.	Cryptocurrency or other anonymous or unverified payment methods.
Adverse Media	No negative information identified.	Questionable or unverified reports of misconduct.	Confirmed involvement in criminal or illicit activities.

Guidance on Using the Risk Indicators

These indicators serve as practical tools for onboarding and monitoring teams to assign risk classifications. During client onboarding and throughout the customer lifecycle, each risk factor should be reviewed separately and then collectively assessed to determine the appropriate risk level.

Where the majority of indicators point toward a low-risk profile, the customer may be processed using standard due diligence procedures.

If the customer shows a mix of low and medium-risk characteristics, enhanced checks are introduced, and monitoring is increased accordingly.

For customers who demonstrate one or more high-risk traits, Enhanced Due Diligence (EDD) is required before account activation, along with authorization from senior management. These clients also undergo frequent and rigorous monitoring.

All customer risk ratings must be re-evaluated periodically or upon the emergence of new behavioral patterns, external alerts, or regulatory developments. This ensures Infusion Tech B.V. maintains a dynamic and responsive risk assessment framework aligned with evolving threats and compliance obligations.

Onboarding Procedures

Infusion Tech B.V. applies a rigorous, structured, and fully documented onboarding process to ensure that only customers who meet the company's compliance and risk acceptance criteria are granted access to the gaming platform. Customer accounts are not activated until all required identification, verification, and sanctions screening procedures have been successfully completed.

Customer Registration and Identification

During registration, customers are required to provide accurate personal data, including:

- Full legal name
- Date and place of birth
- Nationality
- Residential address
- Official identification number (e.g. passport or national ID)

All customers are screened against international sanctions and Politically Exposed Person (PEP) databases using automated tools. Any potential matches generate alerts that are manually reviewed by trained compliance officers to validate results and eliminate false positives.

Where the customer is flagged as high risk during initial assessment, enhanced verification procedures are implemented. This includes submission of supporting documentation to validate the legitimacy of funds and, where applicable, the source of wealth. Documents may include:

- Recent bank statements showing income deposits
- Tax returns or payslips
- Financial statements
- Asset sale contracts
- Investment statements

These measures ensure regulatory compliance and robust control over potential financial crime risks.

Client Identification and Verification Requirements

This section applies to individuals who directly or indirectly establish a business relationship with Infusion Tech B.V., including beneficial owners and authorized representatives.

Document Verification Objectives

Verification procedures aim to prevent:

- Forgery
- Data tampering
- Identity fraud
- Document manipulation (e.g. screenshots, printouts)

The ID document must contain at least the following:

- Full name
- Full date of birth
- Document number
- Validity date (issue or expiration date)
- Photograph of the owner
- Signature (if applicable)

The ID document must also meet these conditions:

- Valid for at least one month from upload date
- Not damaged or unreadable
- All information must be legible

Upload and Validation of ID Documents

Uploaded ID images must meet the following criteria:

- Original photos or scans in JPG, JPEG, PNG, or PDF formats
- Both front and back uploaded, if applicable
- Minimum resolution of 300 DPI or file size of 100 KB
- Color image
- All document corners visible, no foreign objects
- No image editing or PDF conversion allowed
- No digital-only IDs accepted unless explicitly permitted

Image Authenticity and Integrity Checks

Infusion Tech B.V. uses automated signature analysis to ensure uploaded documents are original and unaltered. This includes analysis of:

- File metadata and compression parameters
- Camera or software-specific tags
- Risk scoring to identify potentially manipulated images

Image integrity is further assessed through:

- Conformity to document templates
- Font and layout compliance
- Presence of required fields

Extracted data is validated through internal systems and external databases.

Proof of Address Verification

Face-to-Face Clients

The Money Laundering Compliance Officer (MLCO) inspects the original Proof of Address (PoA) document and retains a certified copy.

Non Face-to-Face Clients

For remote onboarding, the following process applies:

- Upload of PoA document issued within the last three months
- Image authenticity checks
- Digital trust score assessment
- Template matching for document integrity
- Address verification using external map services such as Google Maps or OpenStreetMap

Supported Proof of Address (PoA) Documents

Accepted documents include:

- Utility bills (electricity, gas, water, internet)
- Bank or credit card statements
- Tax bills or mortgage statements
- Lease agreements
- Voter registration certificates
- Employer certificates
- Public authority correspondence
- House purchase deeds

Alternative documents (only if they include an address):

- Passport
- National ID
- Driving license
- EU residence permit

Note: The same document cannot serve as both ID and PoA.

Non-acceptable documents include:

- Mobile phone bills
- Prepaid card statements
- Medical or insurance bills
- PO Box references

- Expired documents (older than 3 months)

Source of Funds (SOF) and Source of Wealth (SOW)

Source of Funds (SOF) refers to the origin of the funds being deposited or transferred.

Source of Wealth (SOW) refers to the origin of the client's total wealth or financial background.

Documentation to support SOF/SOW includes:

Income Category	Documents Required
Salary	Payslips, tax statements, bank account statements
Inheritance	Probate letters, wills, solicitor confirmations
Gifts/Donations	Notarized letters, gift agreements
Savings	Savings or bank statements
Government Grants	Benefit confirmation, grant approval documents
Dividends/Profits	Dividend notes, audited statements
Loans or Investments	Agreements, transfer confirmations
Sales (property/items)	Contracts, shop reports, shipping docs, customs declarations

These documents must clearly link the source to the transaction and demonstrate legitimacy.

Ongoing Monitoring

Infusion Tech B.V. recognises that client acceptance is not a static event but a continuous process that requires ongoing diligence. It is essential to ensure that a customer's behaviour remains consistent with the risk profile established during onboarding and that any suspicious or anomalous activity is promptly detected and addressed.

To this end, Infusion Tech B.V. employs automated transaction monitoring systems that analyse activity patterns to identify indicators of potential financial crime. Alerts are generated for transactions or behaviours such as:

- Deposits or withdrawals that do not align with the customer's known profile
- Rapid movement of funds with minimal or no genuine gaming activity
- Use of multiple or unusual payment instruments
- Behaviour that may suggest dumping, collusion, or bonus abuse

Each generated alert is reviewed by qualified compliance officers who assess the context and decide whether the matter warrants further investigation or escalation.

In addition to real-time monitoring, Infusion Tech B.V. performs periodic customer reviews on a risk-based schedule. These reviews are used to validate that customer profiles remain accurate and that assigned risk levels are appropriate. If there are significant changes in the customer's circumstances, such as:

- A change in country of residence to a high-risk jurisdiction
- A substantial increase in deposit activity or transaction volume
- Modification in funding sources or payment methods

The customer's risk classification is reassessed. Enhanced due diligence and other appropriate controls are applied as necessary to maintain compliance and safeguard the integrity of the platform.

Prohibited Clients and Transactions

To minimise exposure to financial crime and protect the business from regulatory, reputational, and legal risk, Infusion Tech B.V. enforces strict criteria prohibiting relationships or transactions with specific types of clients and activities.

Client and Transaction Restrictions

It is strictly forbidden to:

- Establish or maintain a business relationship with clients who fail or refuse to provide the required identification and verification documents necessary to build an economic profile, unless a valid justification is provided.
- Enter into business relationships or execute transactions with individuals or entities subject to sanctions under the Company's Sanctions Policy (see Appendix II).
- Conduct business with financial institutions incorporated in jurisdictions lacking a physical presence or meaningful management and that are unaffiliated with any regulated financial group. This includes shell banks or institutions known to permit the use of shell accounts.
- Onboard or transact with individuals or entities directly or indirectly involved in the following criminal activities:
 - Terrorist activities as defined in Directive (EU) 2017/541
 - Narcotics trafficking in accordance with the 1988 United Nations Convention
 - Organised crime under Council Framework Decision 2008/841/JHA
 - Human trafficking and smuggling as outlined in Directive 2011/36/EU
 - Sexual exploitation under Directive 2011/93/EU
 - Fraud against EU financial interests
 - Corruption involving EU or Member State officials
 - Tax-related crimes as defined in applicable national laws
 - Counterfeiting of currency under Directive 2008/99/EC
 - Cybercrime under Directive 2013/40/EU

Other Prohibited Client Categories

Business relationships and transactions are also prohibited with clients:

- Using bearer share instruments
- Operating in the adult entertainment sector
- Engaged in the drug or arms trade
- Listed as Specially Designated Nationals and Blocked Persons (SDNs)
- Acting on behalf of SDNs

- Whose funds or wealth originate from or are linked to sanctioned activity
- Whose source of funds or wealth cannot be verified when required
- Involved in the purchase or sale of virtual assets controlled by sanctioned parties
- Engaging in transactions with third parties owned or controlled by sanctioned parties

Prohibited Jurisdictions

Infusion Tech B.V. does not accept customers residing in or transacting from the following territories or countries, in line with its internal policies and compliance obligations:

Unrecognised or Disputed Territories:

- Crimea
- Republic of Abkhazia
- Donetsk
- Republic of China (Taiwan)
- Luhansk
- Republic of Kosovo
- Nagorno Karabakh Republic
- Republic of Somaliland
- Palestine
- Republic of South Ossetia
- Pridnestrovian Moldavian Republic
- Turkish Republic of Northern Cyprus

Prohibited Jurisdictions and Countries:

- Australia
- Belarus
- Belize
- Central African Republic
- Cuba
- Curaçao
- Democratic Republic of Congo
- Dutch West Indies (Aruba, Bonaire)
- France

- Germany
- Iran
- Iraq
- Lebanon
- Libya
- Mali
- Netherlands
- North Korea
- Russia
- Somalia
- Sudan
- Syria
- Turkish Republic of Northern Cyprus
- United Kingdom
- United States
- Yemen

Customers from these jurisdictions are automatically rejected, and transactions involving them are blocked and logged in accordance with applicable regulatory requirements.

Enhanced Due Diligence (EDD)

Infusion Tech B.V. applies Enhanced Due Diligence (EDD) procedures in cases where a customer presents a heightened level of risk. This includes, but is not limited to: Politically Exposed Persons (PEPs), their close family members or associates; individuals based in or transacting from high-risk jurisdictions; customers whose activity involves unusually large, opaque, or complex financial movements; and those whose declared income or business profile does not align with their transactional behavior.

EDD goes beyond standard due diligence by requiring a more thorough examination of the customer's background and financial situation. This involves obtaining credible and independently sourced documentation that clearly demonstrates both the origin of the customer's funds (Source of Funds) and the overall financial background (Source of Wealth). The review may also include:

- Cross-referencing corporate registry data and public filings to verify legal ownership and control.
- Confirming the customer's employment status or business activities through documented evidence.
- Reviewing financial statements, tax returns, and other documents that reflect financial standing.
- Screening for reputational risks using adverse media searches and public record checks.

Any customer classified as high risk must be reviewed and approved by senior management prior to the establishment of a business relationship. In particularly sensitive or complex cases, the decision may be escalated to the Board of Directors for final approval.

Following acceptance, such customers are placed under a strict enhanced monitoring regime. This includes setting lower thresholds for reviewing transactions, maintaining closer scrutiny of behavioral patterns, and increasing the frequency of risk reassessments to detect any emerging threats.

These efforts ensure that Infusion Tech B.V. maintains effective oversight over high-risk client relationships and operates in full compliance with its legal obligations and internal risk appetite.

Prohibited Categories of Customers

Infusion Tech B.V. enforces a strict exclusion policy against individuals or entities that fall into any of the following categories. The company will not onboard, or will terminate, any relationship involving:

- Customers who are anonymous, use false identities, or fail to complete verification within 30 days.
- Shell companies, fictional entities, or those lacking transparent beneficial ownership.
- Any individual or business listed on international or national sanctions lists, including those issued by the UN, EU, OFAC, OFSI, the Sanctions National Ordinance (SNO), or the Kingdom Sanction Act.
- Clients residing in or transacting from countries or regions that are banned under the company's internal policies or deemed high-risk for financial crime.
- Underage individuals who do not meet the legal gambling age requirements.

- Customers linked to illicit activity such as fraud, identity theft, bonus abuse, or other forms of manipulation.
- Customers using unverified third-party payment methods or anonymous funding channels without justification.
- Any person whose source of funds or wealth cannot be confirmed or is suspected to be tied to criminal conduct.

Triggers for Immediate Rejection or Suspension

Applications or active customer accounts may be immediately declined or frozen upon detection of any of the following triggers:

Identity and Documentation Issues

- Refusal or failure to provide required Know Your Customer (KYC) documents, proof of address, or enhanced verification within established deadlines.
- Submission of forged, altered, or suspicious documentation.
- Non-compliance with 30-day verification timeframes despite follow-up reminders.

AML/CTF/CPF Concerns

- Matches against sanctions or PEP databases that cannot be mitigated through risk-based measures.
- Clear indicators of money laundering, terrorism financing, proliferation financing, or other serious financial crimes.
- Inability to verify the customer's source of funds or wealth following reasonable inquiries.

Behavioural or Transactional Red Flags

- Transactions that are inconsistent with the declared profile, such as disproportionate withdrawals or deposits without legitimate gameplay.
- Use of multiple accounts, suspicious third-party transactions, or payment instruments not registered to the customer.
- Attempts to bypass security controls or conceal financial activity through intermediaries.
- Signs of gameplay manipulation, collusion with other users, or activities designed to exploit bonuses or defraud the platform.

Termination of Customer Relationships

Infusion Tech B.V. retains the right to suspend or permanently terminate any customer relationship when such action is justified by applicable regulations, internal compliance policies, or risk-based determinations. Termination may occur under various circumstances, including:

- Failure to submit required identification documents or complete verification processes within 30 calendar days;
- Reasonable grounds to suspect involvement in money laundering, terrorism financing, or proliferation financing;
- Engagement in activities that violate the law, regulatory requirements, or the company's Responsible Gambling Policy.

In cases where termination is linked to suspected criminal behavior, Infusion Tech B.V. promptly reports the incident to the Financial Intelligence Unit (FIU), in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Unless prohibited by law, any residual funds in the customer's account are returned to the original funding method. Where legal obligations require freezing or seizing the funds, the company will comply fully with enforcement authorities.

All decisions to suspend or terminate a client relationship are documented in detail, including the underlying reasons, supporting documentation, and evidence. These records are maintained securely for no less than five years, in line with applicable recordkeeping obligations.

Termination may also be triggered in the following scenarios:

- The customer resides in or transacts from a jurisdiction that is prohibited or sanctioned;
- Verification or supporting documentation is not provided within the required timeframe;
- Information submitted during registration is found to be false, misleading, or incomplete;
- The legitimacy of the customer's source of funds or wealth cannot be established;
- The customer is implicated in or under investigation for financial crime;
- A PEP classification is assigned, and the risk cannot be sufficiently mitigated;
- Evidence of collusion, abuse of promotional programs, or unauthorized gambling practices is identified;
- Unauthorized use of third-party payment accounts is attempted;
- The customer has been self-excluded or barred due to responsible gambling measures;

- Requests for substantial chip redemptions or withdrawals are made without gameplay justification;
- The individual is found to be underage and below the legal threshold for participation.

Compliance with Curaçao's Legal and Regulatory Framework

The Customer Acceptance Policy forms a core component of Infusion Tech B.V. broader AML, CTF, and CPF compliance strategy. It is designed in full accordance with Curaçao's prevailing laws and supervisory guidelines, including:

- **National Ordinance on Identification when Rendering Services (NOIS)**
- **National Ordinance on the Reporting of Unusual Transactions (NORUT)**
- **Sanctions National Ordinance (SNO)**
- **Kingdom Sanction Act**
- **National Ordinance on Games of Chance (LOK)**

The company integrates these obligations into all operational practices. Customer acceptance processes are not limited to onboarding but extend throughout the client relationship, with ongoing due diligence ensuring that any significant changes in a client's behavior, risk exposure, or jurisdictional status are detected and acted upon promptly.

All employees who are involved in customer onboarding, document review, or client verification undergo targeted training on the relevant legal framework and internal procedures. These training programs ensure that employees can identify risk indicators, escalate complex cases, and apply the company's Risk-Based Approach effectively.

To maintain the effectiveness of its internal controls, Infusion Tech B.V. conducts independent audits at least once annually. These audits assess the implementation of the Customer Acceptance Policy and verify the correct application of processes such as KYC checks, sanctions and PEP screening, and enhanced due diligence procedures. The results are submitted to the Board of Directors, and any shortcomings are addressed through corrective action plans with clear deadlines.

Integration with Responsible Gambling Framework

Infusion Tech B.V. ensures that its Customer Acceptance Policy is fully aligned with its Responsible Gambling Policy, recognizing that preventing gambling-related harm is a core part of its regulatory obligations and ethical responsibilities.

Where customer activity indicates signs of potential harm—such as frequent deposits that appear disproportionate to their known income, or prolonged gaming sessions—the company initiates prompt intervention. Depending on the severity and context, actions may include:

- Applying deposit or loss limits;
- Restricting access to specific services;
- Temporarily suspending the account;
- Imposing a complete account lock to safeguard the customer.

Self-exclusion requests are processed without delay and applied comprehensively to all accounts connected to the customer, ensuring that exclusion measures cannot be bypassed across platforms. These restrictions remain in force for the duration specified by the customer or for as long as legally required.

All frontline and customer support employees receive focused training to help them detect early indicators of problematic gambling. This training is embedded in the onboarding and continuous monitoring procedures, allowing staff to act quickly and refer customers to appropriate interventions where required.

Policy Review and Oversight

This Customer Acceptance Policy is reviewed and updated no less than once per calendar year. The purpose of the review is to:

- Ensure continued compliance with applicable regulatory and legislative requirements;
- Reflect changes in the company's operational model, risk appetite, or product offering;
- Incorporate new risks identified through internal audits or regulatory advisories;
- Align with emerging best practices in the field of AML/CTF/CPF compliance and customer onboarding.

The Compliance Officer is responsible for initiating and conducting the review process. Proposed amendments are documented and submitted for approval to the Board of Directors. Once approved, the updated policy is communicated to all relevant personnel, accompanied by

targeted training to ensure that the revised provisions are implemented effectively across the organization.

Record Retention and Data Protection

Infusion Tech B.V. maintains comprehensive records of all activities related to customer acceptance and verification for at least five years following the conclusion of the business relationship, in compliance with legal obligations.

These records include:

- Personal identification and verification documents;
- Proof of residential address;
- Evidence supporting source of funds and source of wealth;
- Internal risk assessments and due diligence reviews;
- Transaction monitoring alerts and investigation notes;
- Records of Enhanced Due Diligence (EDD) actions;
- Documentation regarding account restrictions, suspensions, or closures.

All records are stored in encrypted formats with access strictly limited to authorized compliance personnel. Access logs are maintained and routinely audited to ensure adherence to internal policies and data protection standards. Infusion Tech B.V. is committed to upholding data security, confidentiality, and privacy in line with applicable laws and best practices.

9. Transaction Monitoring

Infusion Tech B.V. recognises that transaction monitoring is a cornerstone of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework. Within the context of the online betting and gaming sector, where transaction volumes are high and the velocity of financial flows is rapid, the risk of misuse for illicit purposes is elevated. As such, the company operates a robust, technology-enabled transaction monitoring system designed to detect, assess, and respond to suspicious or unusual activity in a timely manner.

Compliance with Curaçao Regulatory Expectations

In alignment with Curaçao's licensing requirements and the guidelines issued by the Financial Intelligence Unit (FIU Curaçao), Infusion Tech B.V. has implemented a comprehensive transaction monitoring mechanism that identifies behaviours or patterns potentially indicative of unlawful activity. The system is designed to ensure compliance with the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), and other applicable laws.

Monitoring Framework and System Functionality

Infusion Tech B.V. employs a proprietary transaction monitoring solution that operates on a real-time basis, combining automated surveillance with manual oversight. The system leverages data analytics and machine learning to flag transactions based on risk thresholds, behavioural anomalies, and financial irregularities. Alerts are automatically generated for further investigation by the Compliance team, with escalation protocols defined for serious or persistent red flags.

The transaction monitoring framework focuses on several high-risk behaviours, including:

- Large or irregular deposits not aligned with the customer's profile
- Multiple payment methods, including unregulated or anonymous channels
- Rapid deposit and withdrawal cycles without genuine gameplay
- Transfers between accounts or suspected linked profiles
- High-frequency transactions from geolocations known for financial secrecy

Risk-Based Parameters and Review Process

The monitoring system assigns risk scores to transactions based on the customer's profile, the value and velocity of the transaction, and the associated payment methods. Alerts are triggered when transactions meet specific criteria or thresholds. These are then reviewed by the AML/CFT Officer or designated team members.

Common monitoring parameters include:

- Transactions equal to or exceeding NAF 4,000 (or equivalent in another currency)
- Patterns of frequent, high-value deposits and withdrawals
- Discrepancies between customer activity and declared source of funds
- IP geolocation inconsistencies and account logins from high-risk regions

For transactions meeting the statutory NAF 4,000 threshold, Customer Due Diligence (CDD) is triggered. If linked transactions cumulatively reach this amount, full verification is required regardless of whether they were performed separately. This includes deposits, bets, and withdrawals.

Monitoring Techniques

Key techniques used in Infusion Tech B.V. transaction monitoring include:

- **Geolocation tracking:** Ensuring access is not attempted from restricted jurisdictions
- **IP address monitoring:** Detecting duplicate or suspicious access patterns
- **Velocity checks:** Identifying rapid transaction flows across accounts
- **Source of funds analysis:** Reviewing documentation for high-value or irregular transactions
- **Behavioural analytics:** Analysing deviations from established gameplay or spending patterns

The system continuously evaluates data such as deposit methods, stake size, betting history, win/loss trends, and time spent gaming. These variables help detect anomalies that could indicate potential abuse or financial crime risks.

Internal Escalation and Reporting Protocols

When suspicious activity is identified, an internal Suspicious Activity Report (SAR) is submitted by the first line of defence to the AML/CFT Officer. If the suspicion is substantiated, the case is reported to the FIU Curaçao in accordance with NORUT requirements. A record of the alert, the investigation process, and any follow-up actions is retained for audit and compliance purposes.

If the required CDD or Enhanced Due Diligence (EDD) measures cannot be completed, the customer's account is frozen. The business relationship is then terminated, and any remaining funds are returned via the original funding method, unless legal grounds exist for seizure or regulatory hold.

10. Politically Exposed Persons

Enhanced Due Diligence (EDD) plays a vital role in safeguarding the online gaming and betting industry from financial crimes such as money laundering, fraudulent schemes, and other

unlawful behavior. EDD represents a more rigorous process of verifying customer identity and assessing background information, particularly in cases involving individuals who present an elevated risk.

Within the context of online gambling, customers considered high-risk typically include those conducting high-value or frequent transactions, displaying irregular betting behaviors, or classified as Politically Exposed Persons (PEPs). A PEP is defined as someone who currently holds or has recently held a high-ranking public position—such as a head of government, senior politician, judiciary member, senior military officer, or an executive in a state-owned enterprise or international organization. The risk profile extends to their immediate family members and close personal or business associates, all of whom must be treated as high-risk.

At Infusion Tech B.V., all customer applications involving PEPs are subject to a heightened level of scrutiny. The process is overseen by senior management, and no business relationship may proceed without their explicit approval. Upon identification, PEP-related applications activate additional compliance controls, which include comprehensive risk evaluation and verification of both the customer's source of wealth and source of funds.

To ensure continuous oversight, the Compliance Officer maintains an internal register that records all identified PEPs and related risk assessments. This log is periodically reviewed to ensure ongoing accuracy and to reflect any changes in the customer's risk status. By enforcing these measures, Infusion Tech B.V. upholds its regulatory obligations and reinforces its commitment to financial integrity across its platform.

11. Sanctions Policy

Infusion Tech B.V. is committed to complying with all applicable legal obligations relating to international sanctions. This Sanctions Policy establishes the standards and operational controls necessary to identify, prevent, and manage exposure to sanctioned individuals, entities, and jurisdictions. Sanctions are implemented by national governments and international bodies as part of their foreign policy and national security frameworks, aiming to discourage conduct deemed threatening or in breach of international norms.

Sanctions regimes can take various forms, depending on the issuing authority and the objectives pursued. The principal categories include:

- **Comprehensive Sanctions:** Broad prohibitions affecting all trade and financial activity with entire countries or regions, such as the Crimea region. These measures are used to exert economic pressure and restrict access to strategic resources and international markets.
- **Regime-Based Sanctions:** These measures target specific regimes or political leadership, focusing on designated individuals or entities involved in governance or associated with serious misconduct. They are typically accompanied by limited trade restrictions or embargoes and aim to support human rights, rule of law, and anti-corruption objectives.
- **Sectoral Sanctions:** Imposed on critical sectors of a country's economy (e.g., energy, defense, financial services), these sanctions restrict specific activities without completely banning trade with the jurisdiction.
- **Debt and Equity Sanctions:** These limit access to new capital by prohibiting transactions involving certain types of financial instruments. They often apply to state-owned enterprises or businesses linked to strategic industries.
- **Conduct-Based Sanctions:** These list-based sanctions target individuals or organizations engaged in specific unlawful activities such as terrorism, human rights abuses, arms trafficking, cybercrime, organized crime, or large-scale corruption. Designations under these regimes are typically made regardless of nationality or location.

These categories may overlap, and individual sanctions programs may incorporate elements from multiple types.

Relevant Sanctions Frameworks

Given the international nature of its operations, Infusion Tech B.V. is potentially subject to several overlapping sanctions regimes. The company ensures compliance with the following:

United Nations (UN)

Sanctions established by the United Nations Security Council (UNSC) under Chapter VII of the UN Charter are binding on all member states. Infusion Tech B.V. observes UN sanctions as required under international law and reflects these obligations in its internal controls and compliance systems.

European Union (EU)

The EU implements both UN sanctions and its own autonomous restrictive measures under the Common Foreign and Security Policy (CFSP). EU sanctions apply:

- Within the territory of the EU, including airspace;
- To EU nationals, regardless of their location;
- To EU-incorporated companies, including non-EU branches;
- To business transactions with any EU nexus;
- Onboard aircraft or vessels under EU jurisdiction.

Infusion Tech B.V. adheres to all EU-imposed restrictions across its operations, irrespective of geographic location.

United Kingdom (UK)

UK financial sanctions apply:

- Within the UK territory and territorial waters;
- To all UK nationals and incorporated entities, including branches outside the UK;
- To any activity conducted within or partially within the UK.

Infusion Tech B.V. complies with UK sanctions unless such compliance conflicts with binding EU law.

United States (US)

US sanctions fall into two categories:

- **Primary sanctions:** These apply to US persons, US entities, and their foreign branches. In some cases, they extend to foreign entities owned or controlled by US entities or holding US-origin goods.
- **Secondary sanctions:** These may target non-US persons who engage in transactions that, while entirely outside the US, are deemed contrary to US foreign policy or national security interests. These apply particularly under programs related to jurisdictions such as Iran, Russia, or China.

Infusion Tech B.V. complies with US sanctions to the extent permitted by EU and local legislation. Where secondary US sanctions conflict with European Council Regulation (EC) No

2271/96 (the Blocking Statute), the Compliance Officer must escalate the matter to the Directors and Board of Infusion Tech B.V. for formal guidance.

Policy Statement

Under this policy, Infusion Tech B.V. commits to:

- Blocking assets and freezing accounts where required by sanctions laws;
- Rejecting or prohibiting unlicensed financial or commercial transactions involving sanctioned jurisdictions, persons, or entities;
- Terminating relationships with customers confirmed to be under sanctions, irrespective of the legal obligations of the jurisdiction in which the relationship is located. If local law prevents termination, escalation to the Board is mandatory;
- Prohibiting deliberate structuring or concealment of transactions designed to circumvent sanctions regulations.

Enforcement and Consequences

Non-compliance with this policy may result in serious legal and regulatory consequences for Infusion Tech B.V., including penalties, criminal prosecution, or reputational damage. Employees who violate applicable sanctions laws may be personally liable and subject to disciplinary action, including potential dismissal.

All staff are expected to understand and adhere to this policy and report any potential breaches or concerns to the Compliance Officer immediately.

Roles and Responsibilities

Board of Directors

The Board of Directors of Infusion Tech B.V. bears the ultimate responsibility for overseeing the company's compliance with its Sanctions Policy. Their duties include:

- Reviewing and approving the Sanctions Policy at regular intervals or as required by legal or regulatory developments.
- Promoting an organizational culture that emphasizes the importance of sanctions compliance.

- Ensuring that the AML/CTF and sanctions compliance function is adequately resourced, independent, and empowered to perform its duties effectively.
- Receiving and reviewing periodic reports from the Compliance Officer concerning sanctions compliance and associated risks.
- Appointing a suitably qualified Compliance Officer and granting this officer the authority necessary to ensure compliance issues are appropriately escalated and addressed.

Director(s)

The Director(s) are tasked with:

- Reviewing regular reports submitted by the Compliance Officer, particularly those highlighting risks or recommending changes.
- Making final determinations on sanctions-related matters escalated by the MLCO, including those involving legal or jurisdictional conflicts.

Compliance Officer

The Compliance Officer is directly responsible for the implementation and day-to-day management of the Sanctions Policy. Key responsibilities include:

- Conducting sanctions risk assessments on transactions and customer relationships, including verification of supporting documents.
- Proposing revisions to the Sanctions Policy and submitting them for Board approval.
- Ensuring relevant staff are kept informed of changes to sanctions legislation, typologies, and enforcement practices.
- Reviewing customer identification data to confirm completeness and accuracy of information collected during onboarding and throughout the business relationship.

All Employees

Every employee of Infusion Tech B.V. is expected to:

- Understand and comply with the Sanctions Policy, relevant procedures, and applicable regulations.
- Maintain a heightened awareness of the risks posed by sanctioned entities and transactions.

- Promptly report any suspected breaches, suspicious clients, or violations of this Policy to the Compliance Officer.
- Refrain from advising clients on how to circumvent sanctions controls or conceal restricted activities.
- Complete all required sanctions training in a timely manner.

Under no circumstances should any employee engage in discussion or provide advice that could be interpreted as assisting a customer in structuring transactions to evade sanctions.

Sanctions Screening

Infusion Tech B.V. applies sanctions screening processes to both new and existing customers, connected parties, transactions, and relevant third parties. This screening is performed using an external risk management platform that continuously monitors against up-to-date sanctions lists.

When a potential match is detected, the system assigns a status as follows:

- **True Positive:** Full match with one or more entries on a sanctions list.
- **Potential Match:** Name match exists, but confirmation details (e.g., birthdate) are incomplete or the individual is flagged for suspicious behavior.
- **False Positive:** Initial data matches, but further review confirms the individual is not the same person listed.
- **Non-Criminal Match:** Applicant matches a listed individual or entity, but without any criminal implication (e.g., a journalist cited in reports).
- **Unknown:** The applicant's name is incomplete, preventing proper analysis.

Cases marked as True Positive or Potential Match are referred to the Compliance Officer for review. If the applicant is rejected due to a sanctions-related issue, a rejection reason is logged accordingly, such as:

- Sanctions Match
- PEP Status
- Criminal Records
- Adverse Media

Sanctions Lists Screened

The screening process covers a comprehensive range of sanctions lists from globally recognized authorities, including but not limited to:

European Union Sources

- European External Action Service (EEAS)
- CFSP Consolidated Sanctions List (including terrorism, human rights violations, cybercrime)
- Council Regulations targeting Russian entities under EU embargoes

United Kingdom

- HM Treasury – Consolidated List of Financial Sanctions Targets in the UK
- BOE list of capital market restrictions
- Foreign, Commonwealth & Development Office (FCDO) Sanctions List

United States

- Department of Commerce (BIS): Denied Persons List, Entity List, Military End User List
- Department of the Treasury (OFAC):
 - Specially Designated Nationals (SDN) List
 - Active programs include those related to:
 - Iran, North Korea, Russia, Syria, Venezuela, Cuba
 - Cyber sanctions, Global Magnitsky, CAATSA, and others
 - OFAC Consolidated Sanctions List (OFAC-CSL) includes:
 - Foreign Sanctions Evaders (FSE)
 - Sectoral Sanctions Identification (SSI)
 - CAPTA List, NS-MBS, NS-CCMC, NS-ISA Lists

United Nations

- United Nations Consolidated Security Council Sanctions List, encompassing all sanctions regimes imposed by the UN.

All screening is conducted prior to account activation and continues throughout the customer relationship to ensure timely identification of any changes in status or new designations.

Response to Sanctions List Matches

If a customer or transaction is positively matched against a sanctions list, the Money Laundering Compliance Officer (MLCO) will take appropriate measures based on the applicable sanctions regime. Actions may include freezing of assets, rejection of the business relationship, or application of specific financial restrictions such as equity or debt-related limitations. These actions are always assessed within the context of any existing conflicts of law to ensure lawful implementation.

Sanctions Evasion

Sanctions regimes administered by the United Nations (UN), United States (US), and European Union (EU) explicitly prohibit the circumvention of their core provisions. Increasingly, regulators view evasion as an independent violation, warranting its own enforcement. Examples of possible sanctions evasion include:

- An unsanctioned individual purchasing digital assets such as cryptocurrency on behalf of a sanctioned company.
- Clients modifying payment details after an initial rejection to obscure links to sanctioned parties (commonly known as wire stripping).
- A US-based client using a virtual private network (VPN) to mask their location and engage in transactions that would otherwise be restricted.
- Transfers involving intermediaries or “front companies” located in non-sanctioned jurisdictions but acting on behalf of sanctioned entities.

Potential evasion attempts may be detected at various organizational levels, including client onboarding, customer service interactions, transaction monitoring, and ongoing due diligence. All suspected instances must be reported to the Compliance Officer without delay. The Compliance Officer will assess the case and determine whether further escalation to relevant authorities is necessary.

In addition to sanctions screening, the company’s broader AML/CTF controls including transaction monitoring and due diligence processes also serve to detect signs of evasion. When

reviewing high-risk clients under the company's money laundering and terrorism financing risk methodology, the Compliance Officer must also assess the possibility of sanctions evasion.

All findings must be documented in accordance with the company's AML policy, and any suspected or confirmed evasion attempts must be reflected in the compliance reports submitted to executive leadership and the Board of Directors.

Asset Freezing

Asset freezing, also referred to as blocking, is a key enforcement mechanism under most sanctions regimes. When a sanctioned party has a direct or indirect interest in an asset, the company is obligated to freeze it. Ownership rights are not transferred, but the sanctioned party is prohibited from exercising any form of control or benefit over the asset unless authorised by a competent authority.

In the context of Infusion Tech B.V., assets include both fiat currency and cryptocurrency. Freezing applies immediately upon confirmation of a sanctions match and restricts any further transactions involving the affected funds.

Sanctions Compliance Training

Sanctions training is a core element of the company's compliance programme. It is the Compliance Officer's responsibility to review and update the training content as necessary to reflect changes in regulatory expectations, risks, or company operations.

There are two levels of training:

1. **Annual general training:** Delivered to all employees to ensure basic knowledge of sanctions obligations and awareness of risk.
2. **Risk-based or role-specific training:** Delivered to employees in high-risk roles, such as those handling customer transactions, onboarding, or payment processing.

New hires must receive training within 30 days of joining the company. Training must cover:

- Major sanctions regimes (UN, EU, UK, US)
- Common sanctions programs and legal requirements
- Examples of sanctions evasion
- Red flags and risk indicators

- Roles and responsibilities of staff
- Legal and operational consequences of non-compliance

Training materials, assessments, and attendance records must be retained in accordance with the company's record-keeping obligations.

Outsourcing of Sanctions Compliance Activities

If any sanctions-related processes are outsourced to external parties, Infusion Tech B.V. remains fully accountable for ensuring such activities meet all legal requirements and comply with this policy. The company must conduct due diligence on service providers and maintain oversight to confirm ongoing compliance.

Record-Keeping and Retention

All sanctions-related documentation must be retained in alignment with the company's AML policy. This includes screening results, investigation records, training documentation, internal reports, escalation logs, and any correspondence with regulatory bodies. Records must be stored securely and remain accessible for at least the minimum period required by law.

12. Suspicious & Unusual Activity & Transaction Reporting

For Infusion Tech B.V., the reporting of suspicious activities within the online betting and gaming sector is a key obligation under both domestic and international anti-financial crime regulations. These reports are essential to maintaining the integrity of the platform and preventing misuse for illicit purposes such as money laundering, terrorist financing, fraud, or corruption.

Submitting timely and accurate reports serves multiple vital objectives. Beyond meeting legal and regulatory obligations, it protects customers from potential exploitation, strengthens trust in the platform, and reduces the risk of reputational damage and regulatory penalties. A failure to report suspicious activity, whether deliberate or due to oversight, can lead to serious consequences, including legal sanctions and criminal prosecution.

Suspicious activity may be detected through irregular transaction patterns or anomalous customer behavior. Examples include unusual deposit and withdrawal structures, drastic changes in account use, excessive wagering that does not reflect typical behavior, or signs that the

customer is indifferent to gaming outcomes. These behaviors might signal financial crime or simply require further scrutiny to rule out underlying risks.

Infusion Tech B.V. uses a two-stage review process. First, flagged transactions or activities are evaluated to determine whether they are abnormal or indicative of possible criminal intent. If suspicion remains, a formal internal report is prepared and submitted to the designated AML/CTF Officer, who assesses whether a report must be filed with the Financial Intelligence Unit (FIU) of Curaçao.

In accordance with Article 1 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), online gambling entities must submit Unusual Transaction Reports (UTRs) via the official goAML portal. This requirement has been in force since 1 January 2021. If an activity qualifies for external reporting, the nominated officer must file it directly through the portal, following the company's internal AML/CTF protocols.

Pending review or upon submission of a report, the relationship with the customer may be temporarily restricted or permanently terminated if the concerns warrant such action.

Internal Reporting Obligations

All employees of Infusion Tech B.V. are obligated to file internal reports if they have knowledge, suspicion, or a reasonable belief that a customer may be engaging in money laundering or terrorist financing. Upon receiving such a report, the AML Officer evaluates the case and determines whether it meets the threshold for escalation to the FIU.

12.1. Suspicious & Unusual Activity

Indicators of suspicious activity may involve both transaction patterns and customer profile irregularities, such as:

- Repeated use of anonymous funding methods (e.g., prepaid cards or vouchers)
- Conflicting geolocation data compared to the origin of funds
- Large deposits followed by swift withdrawals with minimal gameplay
- Use of third-party payment instruments for withdrawals
- Refusal to complete identity verification steps or reliance on proxies
- Declared financial standing inconsistent with observed spending
- Frequent or unexplained changes to account ownership

- Hesitation or refusal to provide due diligence documentation

All such observations are logged in detail, including relevant dates, transaction methods, amounts, and associated customer information. The compliance and anti-fraud teams document and assess the full customer profile for further review and, if required, disclosure.

12.2. Suspicious & Unusual Transactions

An unusual transaction is one that deviates significantly from the customer's established behavior or expected financial activity, particularly where there is no clear legal or economic justification. Infusion Tech B.V. considers the following examples relevant:

- Sudden, unexplained deposits or withdrawals
- Transactions involving new or unrelated third parties
- Financial behavior misaligned with the customer's known or declared income

The company's automated monitoring platform continuously scans for such anomalies. Any alerts generated are escalated to the Compliance Officer. Employees are trained to identify both behavioral and financial red flags and escalate their findings through the designated internal channels.

Categories of Noteworthy Transactions

Certain transaction types require increased scrutiny:

- Transactions previously reported to authorities for potential ML or TF links
- Dealings involving individuals or organizations listed under the Sanctions National Ordinance or similar frameworks
- Any single or linked transactions in a single day amounting to 5,000 Netherlands Antillean Guilders (NAF) or more, regardless of transaction type

Wherever there is reasonable suspicion that a transaction may be connected to money laundering, terrorist financing, or proliferation financing, it must be escalated without delay.

12.3. Timely Reporting

Upon establishing that a transaction is unusual or suspicious, Infusion Tech B.V. must file a UTR with the FIU Curaçao immediately, as required by AML Regulation IV.1. This obligation applies even if the transaction is not completed or was merely attempted.

The Compliance Officer submits the report without needing additional sign-off. Prompt reporting is essential, as delays may result in non-compliance with regulatory requirements.

12.4. Confidentiality & Commitment to the Strong Reporting Culture

Strict confidentiality must be maintained around the SAR and UTR processes. Employees are prohibited from sharing any information regarding the existence or contents of a report with the subject of the report or any unauthorized party.

Disclosing such information could be interpreted as tipping-off, which is a violation of Curaçao's legal standards and can compromise active investigations. Only the Compliance Officer and specifically authorized personnel may access information pertaining to suspicious transaction reports.

To maintain compliance, Infusion Tech B.V. includes dedicated training on SAR confidentiality and reporting obligations as part of its AML/CTF staff training. Any breach of these protocols is treated as a major compliance failure and may result in disciplinary action, including termination.

Commitment to a Strong Reporting Culture

Infusion Tech B.V. is committed to fostering a reporting culture based on vigilance, confidentiality, and accountability. This approach strengthens the company's AML/CTF/CPF framework, ensures compliance with local and international standards, and supports global efforts to prevent financial crime in the gambling sector.

13. Compliance Officer

The Compliance Officer, also referred to as the Money Laundering Reporting Officer (MLRO), holds a central position within Infusion Tech B.V. and is tasked with overseeing the implementation and enforcement of all Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) obligations. This role is

instrumental in maintaining the integrity of the compliance function and ensuring regulatory adherence at all times.

The Compliance Officer acts as the authorized point of contact for all communications with regulatory and supervisory bodies in Curaçao. This individual also supervises the AML Compliance Team, manages daily compliance activities, and ensures the consistent application of the company's age verification controls, responsible gambling safeguards, and self-exclusion measures to prevent gambling-related harm.

To maintain independence and objectivity, the Compliance Officer operates autonomously, free from involvement in commercial or operational decisions. The Compliance Officer has full and unrestricted access to all relevant internal systems, customer data, transaction records, and personnel required to carry out their duties effectively. The position reports directly to the Board of Directors and is granted the necessary authority and resources to manage the AML/CTF/CPF framework in accordance with Regulation V.3 of the CGA AML Guidelines. This reporting structure ensures that compliance issues are escalated promptly to the highest level of governance without conflict of interest.

In addition to overseeing internal controls, the Compliance Officer is responsible for filing reports of suspicious activity with the Financial Intelligence Unit (FIU) of Curaçao. These reports are submitted through the designated goAML platform in accordance with applicable legislation. The officer also prepares and submits quarterly AML/CTF compliance reports to the Board of Directors, outlining key developments, identified risks, and any proposed improvements to the compliance program.

Key Duties and Responsibilities

The Compliance Officer's main responsibilities include the following:

1. Policy Oversight and Implementation

- Leads the application of the company's AML/CTF/CPF policies and procedures.
- Ensures internal practices remain in alignment with evolving legal and regulatory requirements.
- Coordinates updates and revisions to the AML policy framework as needed.

2. Central Coordination of AML Compliance

- Acts as the main point of contact for all AML-related inquiries, both internally and externally.
- Serves as liaison with the FIU, regulators, and law enforcement agencies on compliance matters.

3. Transaction Monitoring and Reporting

- Oversees the continuous review of customer transactions to detect unusual or suspicious patterns.
- Evaluates internal reports of suspicious activity and determines whether to escalate the matter to the FIU.
- Ensures accurate documentation and retention of Suspicious Activity Reports (SARs) and internal alerts.

4. Staff Training and Awareness

- Designs and delivers a structured AML training program for all relevant employees.
- Ensures staff are regularly informed of their obligations under the AML framework and trained to detect red flags.
- Updates training materials to reflect legal changes, enforcement trends, and internal procedural updates.

5. Regulatory Engagement

- Responds to requests from regulatory authorities, auditors, and law enforcement in a timely and accurate manner.
- Participates in official inspections, assessments, and audits as required by law or supervisory bodies.

6. Periodic Internal Audits

- Conducts scheduled assessments of the AML/CTF control framework to identify areas of improvement.
- Implements corrective actions to address weaknesses and prevent future compliance breaches.

7. Record-Keeping and Documentation

- Maintains detailed records of all compliance activities, including SAR filings, internal risk assessments, staff training logs, and communications with authorities.
- Ensures all documentation complies with data protection rules and is readily accessible for regulatory review.

By fulfilling these responsibilities, the Compliance Officer ensures that Infusion Tech B.V. maintains a robust and effective AML compliance framework. This role is essential to safeguarding the company from exposure to financial crime, promoting transparency, and upholding the integrity of Curaçao's gaming and financial services ecosystem.

14. Senior Management

Senior management at Infusion Tech B.V. plays a vital role in maintaining an effective AML/CTF/CPF compliance framework. The Board of Directors mandates active participation from senior leadership in evaluating the company's exposure to inherent money laundering, terrorist financing, and proliferation financing risks. It is the responsibility of the appointed AML/CFT Officer to provide the Board with regular updates on any material issues affecting the control environment, as well as to submit an annual report outlining the effectiveness of the systems and controls implemented to mitigate financial crime risks.

In addition, senior management supports quarterly policy reviews that are informed by the outcomes of monthly risk assessments. Where gaps or weaknesses in internal controls are identified, the AML/CFT Officer may propose changes to the policy and seek the Board's formal approval to address any deficiencies.

Policy Review and Risk-Based Adjustments

Senior management is accountable for ensuring that all relevant AML/CTF/CPF policies and procedures undergo thorough review at least once per year. These reviews are informed by the results of the monthly risk assessments, enabling management to detect control failures and operational vulnerabilities early. Where changes are needed, the AML/CFT Officer may initiate proposals for policy updates, which are subject to Board approval. This process ensures the company's internal controls and risk mitigation strategies remain effective and current.

Oversight of Employee Training

The leadership team is also responsible for the development and supervision of training programs across the organization. These training efforts aim to strengthen awareness of AML/CTF/CPF risks and equip employees with the knowledge and tools necessary to identify suspicious behavior. Special focus is placed on ensuring that staff in high-risk functions are trained to perform their roles in compliance with the company's risk management framework.

Internal Control Environment

Senior management ensures that a strong internal control environment is maintained across Infusion Tech B.V. This includes enforcing proper segregation of duties, establishing approval hierarchies, and conducting ongoing monitoring to identify unusual activity or control failures. Clear documentation of processes and decisions is maintained to support regulatory compliance and operational accountability.

To provide assurance that the AML/CTF/CPF program remains effective, independent audits and internal assessments are conducted regularly. These evaluations help senior management identify opportunities for improvement and ensure the company's risk controls continue to meet the requirements set forth under Curaçao's AML legislation and the guidelines issued by the Curaçao Gaming Authority.

15. Employee Training & Screening

Employees play a frontline role in the implementation of AML and CTF controls in the gambling and betting industry. At Infusion Tech B.V., the company maintains a strong culture of ethics and regulatory compliance, which includes carefully screening employees and providing structured, role-specific training to support its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) program.

To safeguard operational integrity, the company implements an Employee Screening Program aligned with Regulation V.4 of the CGA AML Guidelines. This program is applied both during recruitment and throughout employment, particularly for roles involving financial transactions, customer onboarding, and compliance oversight.

Pre-Employment Screening

Before hiring new personnel, particularly those in compliance-sensitive or client-facing roles, Infusion Tech B.V. conducts several vetting steps to verify the individual's integrity and qualifications. These include:

- Verification of identity and eligibility to work using valid government-issued documentation
- Criminal background checks to assess any past involvement in financial crimes or misconduct
- Employment history verification and reference checks to confirm experience and reliability
- Screening against global sanctions and Politically Exposed Persons (PEP) lists using trusted third-party tools

If a candidate fails to meet the company's integrity criteria or presents a compliance risk, they are not eligible for employment.

Ongoing Employee Screening

Following recruitment, employees in roles linked to AML/CTF responsibilities continue to be monitored to ensure they remain suitable for their positions. This includes:

- Annual re-screening of employees in risk-sensitive roles
- Screening triggered by specific events such as internal investigations, disciplinary actions, or job role changes
- Monitoring for changes in sanctions exposure, legal risk, or PEP status

All results from employee screening processes are stored securely and retained for at least five years, in accordance with data protection and regulatory requirements.

AML Training and Staff Awareness

All relevant employees receive training on AML/CTF compliance during onboarding and are required to attend refresher sessions annually. This training is tailored to the specific duties of each department and is designed to ensure employees understand:

- The company's legal obligations under the AML/CTF/CPF framework

- How to identify and respond to suspicious behavior or transaction patterns, such as:
 - Large, irregular betting activity
 - Discrepancies in deposit and withdrawal behavior
 - Use of anonymous or third-party payment methods
- The process for submitting a Suspicious Activity Report (SAR)
- The need to protect client confidentiality and adhere to data protection standards

Employees are made aware that failing to comply with AML or CTF obligations, including failure to report suspicious activity, may result in disciplinary action, legal consequences, or criminal prosecution.

Reporting Suspicious Activity

When an employee identifies unusual or potentially suspicious behavior, they are required to escalate the matter immediately to the Compliance Officer. This is done through the company's internal reporting system and involves completing a Suspicious Activity Report (SAR). Employees are trained on this process and are reminded of the importance of acting without delay.

Data Protection and Confidentiality

All staff are trained to understand and respect the confidentiality of AML-related reports and internal investigations. Information about potential violations is handled in strict confidence and shared only with the Compliance Officer or other designated personnel. Any breach of confidentiality or data misuse is treated as a serious policy violation.

16. AML Compliance Audit

Infusion Tech B.V. recognizes the pivotal role of internal audits in maintaining the integrity, effectiveness, and ongoing alignment of its Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance system. These audits are not treated as routine procedures, but as key elements of corporate governance that promote accountability and operational resilience. All audit findings are formally reported to senior management and the Board of Directors to ensure timely oversight and action.

To uphold the highest compliance standards, the company performs AML compliance audits on a periodic basis, with a minimum frequency of once per year. Additional audits are conducted when there are major regulatory updates, significant internal changes, or incidents that raise compliance concerns. These reviews are led by qualified internal or external professionals who are independent from day-to-day compliance operations and have specialized knowledge in financial crime prevention.

Audit Scope and Focus

Each audit assesses the strength and execution of the AML framework, with emphasis on the following areas:

- **Policies and Procedures Review:** Verifies that AML/CTF/CPF policies are current, meet regulatory obligations, and are implemented effectively throughout the organization.
- **Risk-Based Approach Evaluation:** Examines the methodologies and execution of Business Risk Assessments (BRA), Customer Risk Assessments (CRA), and related controls.
- **Transaction Monitoring and SAR Processes:** Assesses the adequacy of transaction surveillance systems and the accuracy and timeliness of suspicious activity reporting.
- **Customer Due Diligence (CDD) and KYC/KYB Compliance:** Conducts file reviews to confirm that identification, verification, and beneficial ownership measures are properly applied and documented.
- **Sanctions Screening Effectiveness:** Verifies the operation and accuracy of tools used for screening against domestic and international sanctions lists.
- **Employee Training and Screening:** Evaluates whether staff training requirements and screening protocols are being adhered to in accordance with the company's AML obligations.
- **Technology and Data Integrity:** Reviews IT infrastructure and automated systems used to support AML compliance, focusing on risk scoring, data accuracy, and access control mechanisms.

Reporting and Follow-Up

All audit results are compiled into comprehensive reports and submitted to senior management and the Board in line with the expectations of CGA AML Regulation Section V.7. These reports

highlight any gaps, non-conformities, or control deficiencies, along with detailed recommendations for corrective action and proposed implementation timelines.

In cases where significant deficiencies or compliance risks are identified, the findings are escalated immediately to the Compliance Officer and the Board. Follow-up audits are carried out to ensure that remediation measures are implemented effectively and within the specified deadlines.

Documentation and Regulatory Access

Infusion Tech B.V. retains all documentation related to AML audit activities for no less than five years. These records are securely maintained and made readily available to the Curaçao Gaming Control Board (GCB) upon request. This commitment reflects the company's broader dedication to transparency, regulatory cooperation, and the continuous improvement of its financial crime risk management program.

17. Regulatory Access & Cooperation

Infusion Tech B.V. fully acknowledges the oversight authority of the Curaçao Gaming Control Board (GCB) and other competent regulatory or enforcement bodies. The company is committed to transparent and cooperative engagement with all supervisory examinations and compliance assessments, recognizing such interaction as fundamental to maintaining regulatory trust and operational integrity.

To support this commitment, Infusion Tech B.V. grants full and immediate access to its systems, data, processes, and personnel for the purpose of evaluating its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) controls. This access extends to both scheduled and ad-hoc inspections and includes, but is not limited to, the following categories of information:

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) documentation
- Transaction monitoring data and historical payment records
- Internal and external AML/CTF/CPF risk assessments
- Written policies, procedures, and control manuals
- Compliance communications and training materials
- Logs of suspicious activity reports (SARs) and internal escalations

- System audit trails and compliance-related platforms

The company also facilitates remote and on-site access as required, including live system walkthroughs, technical demonstrations, and the submission of supplementary information or clarification upon request.

All requested documentation is made available promptly and is retained in accordance with applicable record-keeping laws, with a minimum retention period of five (5) years or longer when required by law. Records are stored securely with appropriate safeguards to prevent unauthorized access or tampering.

Acknowledgement of Regulatory Examination Authority

Infusion Tech B.V. acknowledges the examination powers of the Curaçao Gaming Control Board (GCB) as prescribed in Section V.6 of the CGA AML Guidelines. The company affirms its obligation to fully cooperate with all supervisory assessments, whether scheduled or ad-hoc, and shall provide complete access to its AML/CTF/CPF systems, records, staff, and procedures. The company further acknowledges that the GCB is empowered to evaluate the adequacy and effectiveness of its compliance framework and may take appropriate regulatory or enforcement action where non-compliance or material deficiencies are identified.

This open and responsive posture toward regulatory oversight forms a core component of Infusion Tech B.V. governance model and underscores its broader commitment to compliance, transparency, and the prevention of financial crime within the gaming industry.

18. Internal Audit & Reporting

Infusion Tech B.V. maintains an independent internal audit function to ensure the ongoing effectiveness, robustness, and operational soundness of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) compliance framework. These audits are carried out at least once per year or more frequently, if required due to changes in the company's risk profile, regulatory developments, or significant modifications in operations.

Audits may be conducted either by the company's internal audit team or by an external, independent third-party auditor, as appropriate. This ensures that the audit process remains objective and professionally competent, with no conflicts of interest.

Scope of Audit Activities

The scope of each audit engagement includes, but is not limited to, the following:

- Examination of AML/CTF/CPF policies and procedures to ensure they are current, compliant, and effectively applied
- Evaluation of the design and performance of transaction monitoring tools and sanctions-screening mechanisms
- Verification of the completeness and accuracy of Suspicious Activity Reports (SARs) and related documentation
- Review of customer due diligence and enhanced due diligence processes, including proper application of onboarding protocols and risk assessments
- Assessment of the effectiveness of AML training programs delivered to staff, including review of training content, frequency, and staff engagement
- Inspection of the governance structure, oversight responsibilities, and record-keeping practices in place
- Evaluation of whether internal systems and controls are proportionate to the company's business model and risk exposure, and meet legal and regulatory standards

Reporting and Follow-up

Upon completion of each audit, a formal audit report is prepared. This document outlines the audit methodology, key findings, any identified weaknesses or gaps, and detailed recommendations for remediation. The report is submitted without delay to senior management and the Board of Directors, or to a delegated oversight body, where applicable.

Senior management is responsible for ensuring that corrective measures are promptly implemented to address all identified deficiencies. The implementation process must be monitored to completion, and timelines for each action point are to be clearly documented and followed through.

Compliance with CGA AML Guidelines – Section V.5

In accordance with Section V.5 of the Curaçao Gaming Authority's AML Guidelines, Infusion Tech B.V. maintains an independent audit function to evaluate the design, implementation, and effectiveness of its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML/CTF/CPF) framework.

This function is carried out by qualified personnel who are independent from daily compliance operations and possess the necessary expertise in financial crime risk management. The purpose

of this audit is to test whether internal policies, procedures, and controls are appropriately designed and operating effectively in practice.

Findings of each audit are formally documented and reported directly to the Board of Directors, and appropriate remedial actions are implemented and tracked to resolution. The audit scope includes, but is not limited to:

- Risk-based approach methodology (BRA, CRA)
- Customer due diligence and EDD implementation
- Transaction monitoring and reporting systems
- Suspicious activity reporting processes
- Sanctions screening tools and procedures
- Staff training and awareness programs

Audit documentation is retained for a minimum of five (5) years and made available to the Curaçao Gaming Control Board upon request.

Documentation and Retention

All records related to internal audits, including reports, working papers, supporting evidence, and corrective action logs, are securely stored and safeguarded against unauthorized access or alteration. These records are retained for a minimum of five years, or longer where legally mandated.

To ensure effective execution of audit responsibilities, the internal audit function is granted full and unrestricted access to all company systems, personnel, and records required to carry out its duties in line with applicable laws and regulatory expectations.

19. Record-Keeping

Infusion Tech B.V. adheres strictly to legal and regulatory requirements regarding the retention and management of records, ensuring a complete audit trail is available when required by law enforcement or regulatory bodies. In accordance with applicable data protection laws, all records are stored in electronic format for a minimum of five years, starting from the date a business,

commercial, or professional relationship is established with an employee, customer, or third party.

To ensure robust compliance with AML/CTF/CPF obligations, the company has implemented structured procedures for maintaining and securing critical documentation. This includes:

- Verified client identification data and due diligence files
- Complete transaction histories and related correspondence
- Internal Suspicious Activity Reports (SARs)
- Staff AML/CTF training logs and participation records
- Internal and external audit results related to the AML framework

All documentation is stored using secure, encrypted systems with strict access controls in place. Access to these records is limited to authorized personnel only, and all access activity is logged and periodically reviewed. Regular system audits are carried out to verify the accuracy, completeness, and security of the stored data.

20. Appendices

Appendix 1: Customer Risk Calculator

Customer Risk Calculator



NEW total score:	0.00
NEW risk level:	Low
Onboarding specialist:	
Last update date:	

Category	Score
low	0-1.9
medium	1.9-2.9
high	2.9 or more
unacceptable	At least 1 unacceptable

Client no.:	
Name:	

Risk Category	Question	Risk score	Risk level	Additional comments
Client	Customer's Age			
	Customer's Citizenship			
	Customer's Second Citizenship			
	Customer's Country of Birth			
	Customer's Country of Residence			
	Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)?			
PROFILE				
Client	Purpose of account registration?			
Client				
Client				
SOFI/SOW				
Client	Source of funds	average		
Client				
Client				
Client				
Client				
Client				
Client	Source of wealth	average		
Client				
Client				
Client				
Client				
INCOMING PAYMENTS				
Transactions	Average frequency of transactions			
Transactions	Expected total value of transactions per period (NAP)			
Transactions	Types of incoming payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
OUTGOING PAYMENTS				
Transactions	Average frequency of transactions			
Transactions	Expected total value of transactions per period (NAP)			
Transactions	Types of outgoing payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
Transactions				
Transactions	Reasons for outgoing payments	average		
Transactions				
Transactions				
Transactions				
Transactions				
BEHAVIOUR				
Products and Services	Please indicate services of interest	average		
Products and Services				
Products and Services				
Products and Services				
Products and Services				

Risk Category:	To be:	Sum:	Weight:
Client	20%	0	
Geography	20%	0	
Products and Services	20%	0	
Transactions	20%	0	
Channels	15%	0	
Other	5%	0	
		0	

BEHAVIOUR			
Please indicate services of interest		average	
Products and Services			
Products and Services			
Products and Services			
Products and Services			
Products and Services			
CONFIRMATIONS			
Channels		average	
Payment Channels			
Third-party Involvement			
Access			
Onboarding			
Adverse media level			
Client			
Manual risk level adjustment based on the expert judgement (±0.5):			Comment regarding manual risk adjustment: Summary of the applicant:
Other			

Appendix 2 Employee Onboarding & Screening Form

This Employee Screening Program outlines the mandatory standards and procedures that govern the vetting, evaluation, and ongoing monitoring of all personnel employed or engaged by Infusion Tech B.V. It has been developed in compliance with Regulation V.4 of the CGA AML Guidelines, which mandates appropriate screening protocols both prior to hiring and throughout the course of employment.

An accompanying Employee Screening Checklist supports this Program and must be completed in all cases to demonstrate adherence to these procedures.

Applicability

This Program applies to:

- All permanent, temporary, and contract-based employees.
- Senior management, the Compliance Officer, and all personnel involved in AML/CTF/CPF responsibilities.
- Individuals engaged via outsourced or third-party arrangements whose roles involve regulated or sensitive tasks.

No individual may begin work in a sensitive or regulated function without completing the required screening measures set forth in this Program.

Screening Requirements

Infusion Tech B.V. ensures that all employees are competent, trustworthy, and suitable for their assigned responsibilities. The screening procedures are proportionate to the sensitivity of the role and must be fully documented.

The screening process includes the following components:

- **Pre-Employment Checks**
- **Fit-and-Proper Assessment** (for designated positions)
- **Ongoing Monitoring**
- **Completion of the Employee Screening Checklist**

1. Pre-Employment Checks

Human Resources, in collaboration with the Compliance Department, carries out the following steps before onboarding:

Criminal History Check

A background check is conducted to identify any convictions for fraud, corruption, financial crimes, money laundering, or other offenses that raise integrity concerns.

Identity Verification

Applicants must present valid government-issued identification documents, which are verified for authenticity and accuracy.

Education and Certification Validation

Academic degrees and professional qualifications relevant to the role must be independently validated.

Employment History Confirmation

Previous job roles, responsibilities, performance, and conduct are verified, subject to local legal requirements.

Reference Checks

At least two professional references are required. Any adverse findings must be referred to the Compliance team for further evaluation.

Pre-employment cannot be finalized until the screening process is completed and the checklist has been reviewed and signed.

2. Fit-and-Proper Assessment

For key roles, a formal assessment is undertaken to determine the individual's fitness for the position, based on the following factors:

- **Integrity and Reputation**

Absence of disciplinary records, regulatory sanctions, or criminal convictions.

- **Professional Competence**

Assessment of technical knowledge, skills, and experience in regulatory or AML functions.

- **Financial Soundness**

Where permissible under local laws, review of financial history including insolvency or bankruptcy.

- **Independence and Objectivity**

Assessment of any actual or potential conflicts of interest.

A completed Fit-and-Proper Assessment Form must be reviewed and approved by the Compliance Department and retained with the screening documentation.

3. Ongoing Employee Monitoring

Annual Rescreening

Employees in high-risk or compliance-related functions undergo periodic rescreening, which may include:

- Updated criminal background checks
- Reassessment of suitability for their role
- Performance and conduct reviews
- Confirmation of continued independence

Trigger-Based Rescreening

Re-screening is required when:

- An employee changes to a sensitive or AML-related role
- Allegations of misconduct emerge
- External developments raise concerns
- Regulatory changes impact the position's risk profile

Continuous Conduct Monitoring

Line managers and the Compliance function must report concerns about employee conduct, integrity, or suitability as soon as they arise.

Each rescreening must be documented in the updated Employee Screening Checklist.

4. Documentation and Retention

Infusion Tech B.V. maintains thorough records of all screening procedures, including:

- Criminal check reports
- Identity and qualification verifications
- Fit-and-Proper evaluations
- Completed screening checklists
- Internal memos, approvals, and notes of concern
- Any remedial actions taken

All screening records are securely stored in compliance with applicable data protection regulations and retained for a minimum of five years, or longer where legally required. Records must be available for inspection by competent authorities upon request.

Roles and Responsibilities

Human Resources

- Administers pre-employment screening
- Ensures all documentation is completed and filed
- Escalates any issues to Compliance

Compliance Officer

- Leads assessments for AML-related roles
- Reviews and approves candidates in sensitive positions
- Verifies compliance with Regulation V.4

Senior Management

- Provides oversight and resources
- Reviews exception requests or concerns escalated by Compliance
- Receives regular reports on screening activities

Compliance and Enforcement

Non-compliance with this Program, including incomplete screening documentation or failure to conduct required assessments, may result in disciplinary action, up to and including termination.

Infusion Tech B.V. certifies that this Program meets the standards established under CGA AML Regulation V.4 and is subject to annual review to ensure continued relevance and regulatory alignment.

New Employee check list

Employee: _____

Starting date: _____

1.	Copy of national Identity card or passport	
2.	Work permit (if needed)	
3.	Proof of Residence	
4.	Certificate of clear criminal record	
5.	Non-Bankruptcy letter	
6.	Reference letter from previous employer	
7.	License/certificates	
8.	CV (Curriculum Vitae)	
9.	Good repute questionnaire	
10.	Diploma of high education	
11.	AML and IOM acknowledgement letter	
12.	Privacy Notice	
13.	Induction & Initial Training Policy/Acknowledgement form	
14.	Employment Agreement	