



Infusion Tech B.V.

120001

Chuchubiweg 17, Willemstad, Curaçao

AML/CTF/CPF POLICY

A handwritten signature in blue ink, appearing to be "A. Constantinou", written over the approval text.

APPROVED BY THE BOARD OF DIRECTORS

29/05/2025

Responsible Compliance Officer:

Haris Constantinou

compliance@infusiontechbv.com

Next Planned Review: May 2026

Contents:

1. Statement	2
2. Senior Management	3
3. Online Gaming Landscape	4
4. Money Laundering	4
5. Terrorism Financing	6
6. Proliferation Financing	8
7. AML/CTF/CPF Risk Assessment	10
8. Customer Due Diligence	15
9. Sanctions Compliance	23
10. Suspicious Activity Reporting	24
11. Compliance Officer Appointment & Responsibilities	26
12. Training	28
13. Audit	29
14. Record Keeping	31
15. Definitions	32

1. STATEMENT

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.

2. SENIOR MANAGEMENT

The senior management of Infusion Tech B.V. plays a critical role in identifying, evaluating, and managing risks associated with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF). To maintain effective oversight, the Board of Directors requires the designated AML/CTF/CPF Officer to regularly report on significant changes, challenges, or issues within the control environment. This officer is also responsible for submitting an annual report evaluating the effectiveness of the company's measures and controls in mitigating risks related to money laundering, terrorist financing, and proliferation financing.

Management is tasked with conducting a comprehensive review of all relevant policies and procedures at least once a year. These evaluations are informed by monthly risk assessments, which help identify vulnerabilities in internal controls or risk management practices. Should deficiencies be discovered, the AML/CTF/CPF Officer is authorized to propose corrective measures for the Board's approval, ensuring continuous improvement in compliance and risk mitigation strategies.

In alignment with international best practices, senior management oversees the development and implementation of robust employee training programs. These initiatives are designed to enhance staff awareness and understanding of AML/CTF/CPF risks, equipping them—especially those in key roles—to identify and respond effectively to suspicious activities.

Management also ensures the company's internal control systems are comprehensive and include clear segregation of duties, defined authorization processes, consistent monitoring, and thorough documentation. To reinforce regulatory compliance and optimize the effectiveness of the AML/CTF/CPF program, regular independent audits and evaluations are conducted to provide impartial insights and identify opportunities for improvement.

3. ONLINE GAMING LANDSCAPE

Infusion Tech B.V., a legal entity established in Curaçao, owns and operates the website <https://1xbet.africa>. 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

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.

5. 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.

6. 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.

7. AML/CTF/CPF RISK ASSESSMENT

Infusion Tech B.V. adopts a risk-based approach (RBA) to tackle the critical threats posed by money laundering (ML), terrorist financing (TF), and proliferation financing (PF). This method ensures that the company allocates resources effectively to mitigate the most substantial risks associated with its operations. With the implementation of the latest Curaçao gaming regulations, this approach is essential for compliance, safeguarding the company's standing in the industry, and maintaining the trust of stakeholders.

The revised Law on Offshore Games (LOK), replacing the National Ordinance on Offshore Games of Hazard (NOOGH), introduces stricter Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) obligations for gaming operators. As part of its compliance, Infusion Tech B.V. is committed to employing a comprehensive RBA to address and manage risks related to these financial crimes.

At the core of Infusion Tech B.V.'s risk management framework is a detailed risk assessment process. This involves an in-depth evaluation of various risk factors, including those

associated with customers, products, services, and geographic locations. Regular risk assessments are carried out to identify vulnerabilities and implement corrective measures where needed.

When assessing customer risk, the company considers factors such as whether customers are politically exposed persons (PEPs), originate from high-risk jurisdictions, or possess complex business profiles. Similarly, product and service risks are analyzed, focusing on items with high transaction volumes, potential for anonymity, or features susceptible to abuse. Geographic risk is assessed by evaluating the risk level of the customer's country or region, especially if it has weak AML/CTF/CPF frameworks or high corruption levels.

Once risks are identified, Infusion Tech B.V. implements tailored mitigation strategies based on the severity of each risk factor. These strategies include enhanced due diligence (EDD) for high-risk customers, sophisticated transaction monitoring tools, and thorough identity verification processes. EDD involves collecting additional details, such as the source of funds and beneficial ownership, for high-risk individuals. Transaction monitoring systems are deployed to detect and alert the company of suspicious activities by analyzing patterns of potential money laundering or terrorist financing. Regular updates and continuous monitoring ensure that the company remains vigilant in identifying and addressing risks as they evolve.

The company also prioritizes accurate record-keeping and timely reporting of suspicious activities. It is committed to maintaining detailed records of customer identification, transactions, and risk assessments, as required by law, to ensure transparency and regulatory compliance.

Adherence to Curaçao's Updated Legislative Framework

Infusion Tech B.V. aligns its practices with the revised LOK framework, ensuring compliance with all AML/CTF/CPF requirements. The company's compliance program incorporates a robust risk-based approach tailored to its operational scope and complexity. Regular training sessions are provided to staff, ensuring that they understand their AML/CTF/CPF obligations and how to manage risks effectively. Independent audits are carried out periodically to assess the performance and effectiveness of the company's AML/CTF/CPF strategies and the application of the risk-based approach.

Infusion Tech B.V. recognizes the unique risks posed by the gambling sector, particularly in relation to money laundering and terrorist financing. The company identifies and mitigates customer risks by conducting comprehensive customer due diligence (CDD) and enhanced due diligence (EDD) for high-risk individuals. Key customer risk factors include irregular income sources, high spenders, and PEPs. Continuous monitoring and profile updates, along with stringent identity verification, are employed to mitigate these risks.

Customer Risk

The company evaluates customer risk by examining factors that could indicate a heightened likelihood of involvement in financial crime. This includes assessing the customer's financial behavior, the transparency of income sources, and potential affiliations with politically exposed persons (PEPs). Customers with multiple or opaque income streams, or those demonstrating inconsistent or high-volume financial activity that is not aligned with their declared profile, are considered higher risk and subjected to enhanced due diligence (EDD).

Clients who maintain multiple accounts or who exhibit spending patterns that significantly exceed their known financial means may attempt to obscure transaction trails, which complicates compliance efforts. Infusion Tech B.V. sets clear transaction thresholds based on typical user behavior to trigger investigative reviews. Low-risk customers generally have a single, documented source of income and a consistent transactional footprint, while higher-risk individuals are flagged for closer scrutiny, including more rigorous KYC documentation and monitoring protocols.

Product, Service, and Transactional Risk Exposure

Certain products and transaction types within the iGaming and digital services sector are more prone to misuse for illicit purposes. Services that allow rapid, high-volume transactions or offer anonymity—such as the use of cryptocurrencies or prepaid instruments—can be exploited to introduce, layer, and integrate proceeds from criminal activities into the legitimate financial system.

Examples of heightened product and transaction risks include:

- Use of gaming or wallet accounts primarily as pass-through mechanisms without active service usage.
- Peer-to-peer fund transfers that bypass conventional financial monitoring systems.
- Deposits or withdrawals made using third-party financial tools, including bank accounts or cards not registered to the account holder.

To counter these risks, Infusion Tech B.V. monitors all platform-based transactions in real time and uses automated detection systems to flag atypical behavior. Where red flags are identified, the company initiates investigative protocols and applies EDD measures to assess potential threats.

Geographical Risk Considerations

Geographic risk is assessed by evaluating the customer's country of residence or the origin of their financial resources. Certain jurisdictions are associated with weak AML/CTF enforcement, high levels of public corruption, or a history of non-cooperation with international regulatory bodies. Engagement with clients or transactions linked to these jurisdictions poses an elevated compliance concern.

Infusion Tech B.V. relies on guidance from internationally recognized bodies to evaluate and respond to geographic risks, including:

- FATF list of jurisdictions under increased monitoring or subject to countermeasures.
- Regional reports from the Caribbean Financial Action Task Force (CFATF).
- U.S. State Department International Narcotics Control Strategy Reports (INCSR).
- The European Commission's list of high-risk third countries.
- OFAC sanctions databases and the Transparency International Corruption Perceptions Index (CPI).

Based on these sources, the company categorizes countries into varying levels of risk. Clients from high-risk jurisdictions are subjected to strict onboarding controls and enhanced monitoring, while transactions involving sanctioned countries are blocked or escalated for additional review. Geographical risk profiles are revisited regularly to ensure the company's controls remain responsive to global developments.

Distribution Channel Risk and Authentication Controls

The methods through which Infusion Tech B.V. establishes and manages customer relationships also influence its exposure to financial crime. Channels that permit remote or anonymous access, especially without sufficient verification layers, are inherently more susceptible to misuse. This is particularly relevant in digital environments where face-to-face interaction is absent.

To reduce this risk, the company employs secure identity verification protocols for all customers. These include biometric checks, multi-factor authentication, and identity validation tools that interface with global databases. By ensuring that access to services is tightly controlled and all interactions are traceable, Infusion Tech B.V. maintains operational integrity and regulatory compliance.

Technological Developments Risk Assessment

Infusion Tech B.V. recognizes that continuous technological evolution presents both opportunities and risks within the digital services and iGaming ecosystem. In line with its commitment to regulatory integrity, the company proactively safeguards its operations against the misuse of emerging technologies for illicit financial activities, including money laundering (ML) and terrorist financing (TF). A forward-looking risk management framework ensures that innovation does not come at the expense of security or regulatory compliance.

Risk Identification and Evaluation Procedures

To prevent the exploitation of new technologies, Infusion Tech B.V. conducts structured and comprehensive risk assessments prior to the introduction of any digital tool, platform feature, or operational change. These assessments are essential in evaluating the potential for

financial crime vulnerabilities and ensuring that regulatory obligations under AML/CTF/CPF regimes are met.

Risk assessments are systematically performed under the following circumstances:

- When launching a new product, feature, or service within the platform.
- When implementing new operational procedures designed to improve efficiency or enhance user engagement.
- When introducing new delivery mechanisms, including digital account access, mobile wallet integrations, or alternative payment solutions.
- When adopting or integrating innovative technologies such as blockchain applications, AI-driven tools, machine learning analytics, or enhanced cybersecurity protocols.

Each assessment involves a detailed analysis of potential risk vectors, with a focus on identifying how the technology may be misused to obscure the origin of funds, circumvent due diligence, or exploit system vulnerabilities. All findings are documented and retained to ensure traceability and transparency in line with domestic and international compliance standards.

Implementation of Mitigation Strategies

Where technological risks are identified, Infusion Tech B.V. takes immediate action to integrate targeted controls. These mitigation efforts are designed not only to prevent misuse but also to support continuous compliance with AML/CTF regulations in an evolving threat landscape.

Key mitigation measures include:

- **Strengthening security infrastructure**, such as deploying multi-factor authentication (MFA), biometric identification, advanced data encryption, and AI-based fraud detection technologies.
- **Enhancing monitoring capabilities**, ensuring that transaction surveillance systems can detect and escalate anomalies in real time—especially those reflecting structuring, layering, or uncharacteristic activity patterns.
- **Adapting compliance policies** to reflect the risks posed by digital transformation. The AML/CTF framework is updated regularly to account for emerging crime methodologies and to incorporate new risk indicators tied to technological abuse.

Commitment to Secure Innovation

Infusion Tech B.V. is committed to fostering innovation in a manner that reinforces—not undermines—its compliance posture. The company's approach to technological adoption emphasizes anticipation of risk, continuous system evaluation, and robust internal

governance. Regular reviews of deployed technologies are conducted to reassess vulnerabilities and to adapt mitigation measures as necessary.

By incorporating these risk-based strategies into its AML/CTF/CPF policy, Infusion Tech B.V. effectively mitigates the risks associated with money laundering, terrorist financing, and proliferation financing. The company is committed to upholding Curaçao's regulatory standards while ensuring the integrity and security of the gaming sector.

8. CUSTOMER DUE DILIGENCE

As part of its Customer Due Diligence (CDD) strategy, Infusion Tech B.V. implements strict player identification and verification protocols designed to detect and prevent financial crime risks, particularly those related to money laundering and terrorist financing. These measures are fundamental to ensuring a secure, transparent, and compliant operational environment.

Infusion Tech B.V. is committed to upholding the highest standards in customer due diligence (CDD) to combat money laundering, terrorist financing, and proliferation financing. The company ensures that it does not maintain anonymous or fictitious accounts and verifies the identity of all players. The CDD process is essential for understanding customer behavior, identifying potential risks, and ensuring compliance with both local and international regulations. Any suspicious activity is promptly reported to the relevant authorities, including the Financial Intelligence Unit (FIU) and, when necessary, to the Public Prosecutor's Office.

Infusion Tech B.V. applies CDD measures in the following circumstances:

- Transactions of NAF 4,000 or more.
- Occasional transactions exceeding NAF 4,000.
- When there is suspicion of money laundering or terrorist financing.
- When there is uncertainty regarding previously collected customer identification data.
- When multiple linked transactions exceed NAF 4,000, even if individual transactions are below this threshold.

For high-risk transactions, enhanced due diligence (EDD) measures are applied.

The company's CDD measures are designed to confirm the identity of players and understand their business relationships. The steps include:

- Verifying player identities using legitimate, independent documents or systems.
- Identifying and confirming the ultimate beneficial owner for legal entities and understanding the structure of ownership and control.
- Determining the purpose and nature of the business relationship.

- Performing ongoing due diligence and monitoring player transactions to ensure they align with the company's knowledge of the player and their risk profile, including verifying the source of funds when necessary.

Infusion Tech B.V. ensures confidentiality by not disclosing when a report is made to the FIU, as revealing this could alert the player. In cases of suspected money laundering or terrorism financing, the company may bypass standard CDD processes to file a report directly to the FIU.

Player Identity Verification

To verify a player's identity, the following information is collected:

- Full name.
- Permanent residential address.
- Date and place of birth.
- Nationality.
- Identity number.

In lower-risk situations, only basic details are required. For higher-risk individuals, more comprehensive information is gathered to mitigate potential risks related to money laundering or terrorism financing.

The verification process includes:

- Government-issued photo IDs (e.g., passport, national ID card).
- Supplementary documents such as utility bills or bank statements (dated no older than six months) to confirm the address.
- Additional steps like verifying the address through email or phone and cross-checking the information against reliable databases.
- Biometric checks, IP address tracking, and payment method validation. If insufficient information is provided, the company may request additional steps such as a selfie with the ID or a regulated financial institution's verification of the first deposit.

As part of the CDD process, Infusion Tech B.V. aims to understand the purpose and nature of its relationships with players. While the nature of the relationship may be apparent, the company gathers enough information to identify any unusual or suspicious behavior. For higher-risk clients, the company collects detailed documentation regarding the source of wealth and expected levels of activity, while lower-risk clients may provide basic employment or business details.

Simplified & Enhanced Due Diligence

Infusion Tech B.V. adopts a risk-based approach to customer due diligence, tailoring the depth and scope of its procedures to the level of financial crime risk presented by each customer. This includes the application of Simplified Due Diligence (SDD) where risks are

demonstrably low, and Enhanced Due Diligence (EDD) in scenarios involving higher-risk individuals or complex transactional behavior.

Simplified Due Diligence (SDD)

When a customer is assessed as presenting a low risk of money laundering (ML), terrorist financing (TF), or proliferation financing (PF), Infusion Tech B.V. may apply Simplified Due Diligence procedures. These reduced measures maintain compliance with AML/CTF/CPF regulations while streamlining verification in proportion to the low-risk profile.

Examples of Simplified Due Diligence include:

- Limited data collection – Basic identity information may be sufficient, including:
 - Full legal name
 - Date of birth
 - Residential address
- Deferred identity verification – In clearly low-risk cases, full verification may occur after the customer relationship is established.
- Risk-adjusted verification methods – Where permitted, alternative data sources (without photographic ID) may be used to confirm identity.
- Reduced frequency of updates – For low-risk customers, periodic reviews of identity information and risk profiles may occur less frequently.
- Lower-intensity transaction monitoring – Monitoring thresholds and frequency may be scaled down, provided transactions remain within expected limits.

Limitations of SDD:

SDD is strictly limited to low-risk scenarios and is never applied in cases where:

- There is any suspicion of ML, TF, or PF.
- The customer is classified as high risk (e.g., PEPs, residents of sanctioned jurisdictions, or users of anonymity-enhancing financial tools).

By applying SDD only where justified, Infusion Tech B.V. upholds a flexible but fully compliant approach to risk management.

Enhanced Due Diligence (EDD)

For customers or transactions identified as high risk, Infusion Tech B.V. implements Enhanced Due Diligence measures. EDD provides a more rigorous layer of scrutiny, allowing the company to verify customer legitimacy, detect financial irregularities, and prevent exploitation of the platform.

EDD is applied in the following situations:

- Customers residing in high-risk jurisdictions, particularly those with poor AML/CFT enforcement or subject to international sanctions.
- Individuals identified as Politically Exposed Persons (PEPs), due to their access to public resources and elevated exposure to corruption risks.
- Users transacting with anonymous financial instruments, such as prepaid cards or cryptocurrencies.
- Customers engaging in emerging financial technologies, including blockchain-based services or digital asset transactions.

Key EDD measures implemented by Infusion Tech B.V. include:

- Collection of extended customer information, such as employment status, source of wealth, and historical addresses.
- Comprehensive review of the business relationship, including the purpose and anticipated activity on the account.
- Verification of source of funds and wealth, supported by documents such as payslips, property sale contracts, inheritance certificates, or savings records.
- Detailed scrutiny of transactions, especially those that are unusually large or inconsistent with declared behavior.
- Mandatory senior management approval before initiating or continuing a relationship with high-risk customers.
- Automated high-risk transaction monitoring, with immediate alerts triggered for irregular activity.
- Requirement for the first deposit to originate from a regulated institution, under the customer's own name.
- Periodic re-verification of financial sources for ongoing high-risk clients, ensuring sustained compliance.

By applying SDD and EDD proportionately and consistently, Infusion Tech B.V. ensures that its customer due diligence process aligns with international AML/CTF/CPF standards, supports effective risk management, and reinforces the company's operational integrity and regulatory compliance posture.

Timing of Customer Due Diligence Measures

Infusion Tech B.V. applies Customer Due Diligence (CDD) measures in a timely and systematic manner, in line with its regulatory obligations under Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) frameworks. These procedures are designed to ensure that customer identification, verification, and risk assessment occur at the appropriate stages of the business relationship and in response to specific financial thresholds or behavioral indicators.

CDD Triggers Based on Transaction Thresholds

Upon account registration, the company collects the following minimum customer data:

- Full legal name
- Permanent residential address
- Date of birth
- Politically Exposed Person (PEP) status screening
- Sanctions screening against relevant domestic and international lists

As part of its risk-based methodology, Infusion Tech B.V. ensures that identity verification is completed before the execution of any transaction (or linked series of transactions) equal to or exceeding NAF 4,000.

This threshold-based verification applies to:

- A single transaction that reaches or surpasses the NAF 4,000 limit.
- Multiple linked transactions—including deposits, withdrawals, and peer-to-peer transfers—that cumulatively meet or exceed this value.

To ensure full regulatory compliance, the company monitors transaction activity on a daily rolling basis, calculating total exposure from the start of the customer relationship.

Once the NAF 4,000 threshold is triggered, Infusion Tech B.V. immediately conducts a full risk assessment and completes any outstanding due diligence requirements before allowing further financial activity.

Proactive and Early CDD Implementation

While threshold-based triggers are respected, Infusion Tech B.V. also emphasizes early completion of CDD. As a best practice, full identity verification is performed during the initial account registration phase, even if no immediate financial activity is anticipated. This proactive approach minimizes the risk of the platform being used to funnel illicit funds before proper screening has been applied.

Restrictions on Financial Activity When CDD is Incomplete

To preserve regulatory compliance and platform integrity, Infusion Tech B.V. imposes temporary restrictions when the NAF 4,000 threshold is reached and CDD has not been completed:

- If the threshold is crossed via a deposit: The customer may not make further deposits or withdrawals but is permitted to use any existing funds for gameplay.
- If the threshold is reached due to a withdrawal request: The account is temporarily suspended from both gameplay and transactions until verification is finalized.

Non-Compliance and Escalation Procedures

If a customer fails to submit the required CDD documentation within 30 days of surpassing the NAF 4,000 threshold, Infusion Tech B.V. initiates the following steps:

- The business relationship is terminated.
- If there are grounds for suspecting money laundering or terrorist financing, a **Suspicious Transaction Report (STR)** is filed with the **Financial Intelligence Unit (FIU)**.
- If no suspicion arises, the remaining account balance is refunded to the original payment source (e.g., bank account or e-wallet).
- Where suspicions persist, the company may opt to freeze funds and apply internal escalation procedures in full compliance with AML/CTF rules.

Preventing Tipping-Off Risks

Infusion Tech B.V. recognizes that certain actions—such as freezing an account—could unintentionally alert a customer to an ongoing investigation. To avoid violating anti-tipping-off provisions, the company assesses each case individually, following internal protocols that prioritize discretion while preserving regulatory integrity.

Customer Due Diligence for Existing Clients

Infusion Tech B.V. maintains a continuous commitment to the integrity of its Customer Due Diligence (CDD) processes, extending these measures beyond initial onboarding to encompass the full duration of each client relationship. In line with its risk-based approach to AML, CTF, and CPF compliance, the company routinely evaluates existing customer profiles to ensure they remain accurate, up to date, and reflective of the individual's transactional behavior and associated risk level.

Ongoing CDD Review and Compliance

The company applies ongoing due diligence to all existing customers, combining transaction monitoring with dynamic risk reassessment to capture any significant changes in customer behavior or external circumstances.

For clients whose CDD records were incomplete or outdated at the time of onboarding, Infusion Tech B.V. conducts retrospective verification and implements scheduled updates in accordance with current regulatory expectations. This process is prioritized for high-risk customers or those flagged through internal review mechanisms.

Reapplying CDD to Existing Clients

CDD is reinitiated or upgraded under the following circumstances:

- A material change in a customer's risk profile, such as:
 - Large, unexplained transactions
 - Movement to or from high-risk jurisdictions
 - New classification as a Politically Exposed Person (PEP)
- Updates to national or international AML/CTF regulations requiring refreshed data.

- When a previously verified customer initiates transactions that:
 - Equal or exceed the NAF 4,000 threshold
 - Consist of multiple linked transactions crossing this cumulative value

These triggers automatically require a full risk assessment and the completion of any outstanding CDD obligations.

Managing Legacy Accounts with Incomplete CDD

For customers onboarded before current compliance protocols were fully established, Infusion Tech B.V. undertakes the following steps:

- Applies full CDD procedures, giving priority to those with higher risk indicators.
- Schedules verification reviews at risk-sensitive intervals, ensuring updates are proportional to the customer's transaction behavior and exposure level.

Termination of Business Relationships

Infusion Tech B.V. upholds a strict and transparent procedure for terminating customer relationships that pose an elevated risk of financial crime or fail to meet Customer Due Diligence (CDD) obligations. These measures ensure ongoing compliance with applicable AML, CTF, and CPF regulations while protecting the integrity of the platform.

Grounds for Termination

The company may terminate a customer relationship under the following conditions:

- The individual is found to be engaging in activity suggestive of money laundering (ML), terrorist financing (TF), or other suspicious financial behavior.
- The customer fails to provide the required CDD documentation or refuses to cooperate with verification procedures within a specified timeframe.
- The individual is assessed as posing a high ML/TF risk based on updated risk profiling, behavioral indicators, or jurisdictional exposure.

Termination Procedure

Infusion Tech B.V. follows a controlled and documented process when discontinuing a business relationship:

- Senior management reviews and formally approves all termination decisions.
- A final risk-based review of the customer's account activity is conducted prior to closure.
- If the review identifies unusual or potentially illicit transactions, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU).

- All customer records, including identification details and transactional history, are securely retained for at least five years in accordance with legal and regulatory requirements.

Third-Party Reliance for Customer Due Diligence

Infusion Tech B.V. may utilize third-party service providers to perform specific components of its Customer Due Diligence (CDD) obligations. However, such reliance is governed by a strict regulatory framework to ensure that all processes remain fully aligned with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) requirements. Regardless of any delegation, the company retains full accountability for the proper execution of CDD measures and overall compliance outcomes.

Oversight and Accountability

To ensure transparency and regulatory integrity in third-party collaborations, Infusion Tech B.V. enforces the following controls:

- Formal written agreements are established with all CDD service providers, clearly defining their duties, compliance standards, and data-sharing obligations.
- The company guarantees immediate access to all customer identification records collected by third parties when required.
- Periodic audits and performance reviews are conducted to verify adherence to AML/CTF/CPF protocols.
- Despite any delegation, Infusion Tech B.V. independently determines key compliance factors, such as:
 - The customer's Politically Exposed Person (PEP) status
 - Ongoing risk classification and updates
 - Transaction monitoring and red flag detection

Conditions for Acceptable Third-Party Reliance

To qualify for CDD reliance, the third-party entity must meet specific regulatory standards:

- Must be a regulated institution, supervised under a recognized AML/CFT legal regime.
- Must maintain an independent business relationship with the customer (i.e., not acting solely as an intermediary for Infusion Tech B.V.).
- Must operate in a jurisdiction with equivalent AML/CTF standards, subject to favorable evaluation through the company's jurisdictional risk assessment process.

Infusion Tech B.V. evaluates third-party jurisdictions using internationally recognized intelligence sources, such as FATF mutual evaluations and global AML risk indices, to ensure that outsourcing does not introduce compliance vulnerabilities.

Outsourcing vs. Third-Party Reliance: Key Distinction

Infusion Tech B.V. recognizes the difference between outsourcing and third-party reliance:

- In third-party reliance, the external party conducts specific CDD tasks independently, but the regulatory liability remains with Infusion Tech B.V.
- In outsourcing arrangements, the third party acts under the company's direct instructions, adhering strictly to internal procedures and controls.

Regardless of the structure, Infusion Tech B.V. maintains full oversight and control over customer risk assessments, onboarding decisions, and relationship management.

9. SANCTIONS COMPLIANCE

Infusion Tech B.V. is fully committed to adhering to both international and national sanctions, aligning with regulatory standards to ensure robust compliance with Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) measures. Our policy mandates a comprehensive framework to prevent any transactions with individuals, entities, or regions subject to sanctions imposed by relevant authorities.

A key component of our sanctions compliance is the continuous monitoring of transactions. The company diligently tracks all financial activities to identify any potential violations of sanctions regulations. Any suspicious transactions or activities that may involve sanctioned parties are immediately flagged and reported to the appropriate regulatory bodies.

To further ensure compliance, Infusion Tech B.V. provides ongoing training to its staff. This ensures all personnel remain informed about the latest changes to sanctions regulations and can effectively detect any breaches. This commitment to training reinforces our internal controls, helping us mitigate the risks associated with non-compliance.

To proactively manage sanctions risk, Infusion Tech B.V. uses automated systems that perform real-time screening of all client interactions and transactions against the most up-to-date sanctions lists. Our system is regularly updated with the latest information from national and international authorities to identify and block transactions involving sanctioned individuals, entities, or jurisdictions. If a match or any suspicious activity is detected, the company takes immediate action by reporting the issue to the relevant authorities and, where necessary, freezing accounts or blocking transactions.

Our sanctions compliance procedures are regularly reviewed and adjusted to reflect changes in legislation. The company closely monitors and adheres to the following key sanctions lists:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- GCB Announcements
- European Union (EU) Sanctions
- UK OFSI Sanctions
- United Nations Security Council (UNSC) Consolidated List
- U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Sanctions
- U.S. List of Foreign Terrorist Organizations (FTOs)

These lists are central to the company's efforts to identify potential risks associated with sanctioned individuals, entities, or regions. In case of any suspicious transactions, the company swiftly reports the matter to the relevant authorities and takes corrective actions, such as suspending or blocking transactions and reviewing accounts.

Infusion Tech B.V. is proactive in identifying and preventing any attempts to circumvent sanctions regulations. Through rigorous due diligence processes, we examine indirect or covert actions intended to engage with sanctioned parties or jurisdictions. If any evasion tactics are uncovered, these are immediately reported to the authorities, and necessary actions are taken, including halting transactions and reviewing accounts for compliance.

Regular internal audits and continuous staff training further strengthen the company's ability to detect and respond to any potential violations. These measures help ensure that Infusion Tech B.V. remains in strict compliance with all applicable sanctions legislation, reducing the risks associated with sanctions evasion.

10. SUSPICIOUS ACTIVITY REPORTING

Infusion Tech B.V. maintains a proactive and structured approach to identifying and reporting suspicious activity that may indicate money laundering (ML), terrorist financing (TF), or proliferation financing (PF). This includes behavioral anomalies, significant or unexplained financial movements, and any interaction involving jurisdictions or individuals known to present elevated risk.

All employees are required to remain vigilant and immediately escalate any concerns to the appointed Compliance Officer. Once notified, the Compliance Officer performs a detailed assessment to determine whether further internal action or an external report to the appropriate authority is necessary.

Identifying Unusual Transactions

Transactions are considered unusual if they significantly deviate from a customer's typical financial behavior or profile. Common red flags include:

- Large, unexpected transactions that are inconsistent with known income or gambling activity
- Transfers involving unidentified third parties or high-risk jurisdictions
- Financial operations that lack a lawful or logical purpose

Monitoring tools are used to flag these transactions automatically, with each flagged case escalated to the Compliance Officer for deeper investigation.

Categories of Transactions Warranting Review

In accordance with Curaçao's AML/CTF regulatory framework, Infusion Tech B.V. treats the following types of transactions as unusual and subject to further scrutiny:

- Previously reported transactions: Any transaction already submitted to law enforcement or regulatory bodies due to ML/TF suspicion is immediately categorized as unusual.
- Transactions with sanctioned individuals or entities: Dealings involving any party listed under the Sanctions National Ordinance (N.G. 2014 no. 55) are automatically escalated for further review.
- Transactions at or above NAF 5,000: This applies regardless of payment method—whether via cash, check, electronic transfer, or other digital means.

Examples include:

- Deposits or withdrawals meeting or exceeding the threshold
- Purchases of gaming tokens, credits, or chips above NAF 5,000
- Payouts or redemptions reaching this benchmark

Note: Transactions may be considered collectively if they form part of a linked pattern or series that meets or exceeds the NAF 5,000 threshold in a single gaming day.

Presumptive Suspicion and Escalation

If a transaction shows signs indicative of money laundering or terrorist financing—even without conclusive proof—it must be treated as suspicious and documented accordingly. The

Compliance Officer then evaluates whether it meets the criteria for submission to the Financial Intelligence Unit (FIU).

Maintaining Confidentiality

To safeguard the integrity of the investigation and comply with legal standards, Infusion Tech B.V. enforces strict confidentiality in all matters related to suspicious activity reporting (SAR). Employees are explicitly prohibited from:

- Disclosing SAR-related information to the customer(s) involved
- Discussing the matter with unauthorized colleagues or external parties

Access to SAR documentation and discussions is restricted solely to the Compliance Officer and designated compliance personnel. All employees receive training to reinforce the importance of confidentiality, particularly regarding the risks of “tipping off” and the consequences of non-compliance.

Violations of this policy are treated as serious disciplinary offenses and may lead to termination of employment or other corrective measures.

By cultivating a culture of alertness and discretion, Infusion Tech B.V. reinforces its commitment to regulatory compliance, protects the integrity of its operations, and plays an active role in detecting and disrupting financial crime.

11. COMPLIANCE OFFICER APPOINTMENT & RESPONSIBILITIES

Infusion Tech B.V. appoints a highly qualified individual to serve as the Compliance Officer, a role that is integral to the company's Anti-Money Laundering (AML) strategy. This appointment is made by senior management to ensure the Compliance Officer's independence and authority. The appointed individual is an expert in AML regulations and holds a senior position within the company, ensuring effective oversight of AML policies and procedures. The Compliance Officer's role is formalized through an appointment letter that outlines their responsibilities and the reporting structure within the organization.

Core Responsibilities of the Compliance Officer:

The Compliance Officer is responsible for ensuring that the company's AML framework functions effectively. Their key duties include:

- Policy Oversight: Ensuring the consistent application of AML policies and procedures and their alignment with applicable regulations.
- Point of Contact: Serving as the central point of contact for all matters related to AML compliance.
- Policy Review and Updates: Regularly reviewing and updating AML policies to ensure they reflect current regulatory requirements and emerging risks.
- Training and Education: Overseeing the AML training program to ensure that employees are knowledgeable about AML obligations and their role in maintaining compliance.

Additionally, the Compliance Officer is responsible for:

- Transaction Monitoring and Reporting: Continuously monitoring transactions and customer activities to identify suspicious behavior. The Compliance Officer is responsible for filing Suspicious Activity Reports (SARs) with the Financial Intelligence Unit (FIU) as necessary and keeping detailed records of these reports.
- Policy Development and Revisions: Developing and refining AML policies to ensure compliance with both Curaçao's gaming regulations and international standards. This involves adjusting the company's AML framework to address new risks and regulatory changes.
- Staff Training: Ensuring all employees receive comprehensive AML training, are aware of their obligations, and understand how to detect and report suspicious activities. Training materials are regularly updated to keep pace with any changes in laws or policies.
- Liaison with Regulatory Authorities: Acting as the primary contact for interactions with regulatory bodies, law enforcement agencies, and other relevant authorities on AML matters. This includes responding to information requests and participating in audits or inspections.
- Compliance Audits: Conducting regular internal reviews and audits to assess the effectiveness of the AML program. Any identified deficiencies are addressed, and corrective actions are implemented.
- Record Keeping: Maintaining comprehensive records of all AML activities, including SARs, internal reports, training logs, and policy revisions. These records are kept in compliance with legal requirements and are available for regulatory review.

Through these responsibilities, the Compliance Officer is instrumental in protecting the company from money laundering and terrorist financing risks and ensuring full compliance with Curaçao's AML regulations.

12. TRAINING

Infusion Tech B.V. has established a comprehensive training program designed to equip its employees with the necessary knowledge and skills to detect and prevent activities related to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). The core objective of this program is to ensure that employees are well-informed about their legal obligations, able to recognize suspicious activities, and familiar with the procedures for reporting these behaviors. An informed workforce is critical to the successful implementation of AML/CTF/CPF policies, thereby supporting the integrity of the gaming sector.

Training Program Structure and Scope

The training is tailored to meet the specific needs of various roles within the company, making it relevant for all staff members, including senior management, compliance officers, customer-facing employees, operational teams, and anyone involved in financial transactions or customer interactions.

- Initial Training for New Hires: All new employees undergo thorough onboarding training covering essential aspects of AML/CTF/CPF.
- Refresher Training: To ensure that all employees remain up-to-date with changing regulations and best practices, refresher training sessions are mandatory at least once per year. For roles with higher exposure to AML/CTF/CPF risks, additional training may be scheduled more frequently.

The training program covers the following crucial areas:

- AML/CTF/CPF Laws and Regulations: Employees learn about Curaçao's specific legal requirements for preventing money laundering and terrorist financing, as well as the company's internal policies and procedures to comply with these laws.
- Roles and Responsibilities: Training includes a detailed explanation of each employee's role in ensuring compliance with AML/CTF/CPF regulations.
- Customer Identification and Verification: Employees are trained in customer due diligence (CDD), including the Know Your Customer (KYC) process, and the procedures for verifying customer identities and assessing potential risks.
- Identifying Suspicious Activities: The program educates employees on recognizing behaviors that may indicate money laundering or terrorism financing, and how to report such activities properly.
- Record-Keeping and Legal Obligations: Employees are taught the importance of maintaining accurate records, the legal requirements around data retention, and the consequences of non-compliance.

- Emerging Trends: The training addresses evolving trends in money laundering, terrorism financing, and other financial crimes to help employees stay ahead of potential risks.

To ensure accessibility and effectiveness, the training utilizes a variety of delivery methods:

- In-Person Workshops
- Online Training Modules
- Interactive E-Learning
- Practical Exercises, such as Case Studies and Role-Playing Scenarios

This multifaceted approach caters to different learning styles, reinforcing key concepts and enabling practical application of the training material.

Qualified Trainers and Expert Content

The training sessions are led by qualified professionals with expertise in AML/CTF/CPF regulations. These trainers are either internal compliance officers or external experts who are well-versed in current legal standards and industry practices. Their role is to ensure that the training content remains current, relevant, and accurately reflects any recent developments in AML/CTF/CPF compliance.

Through this robust training program, Infusion Tech B.V. ensures that all employees are fully prepared to prevent money laundering, terrorist financing, and proliferation financing, maintaining a strong compliance culture within the company.

13. AUDIT

To ensure compliance with the latest gaming regulations in Curacao, Infusion Tech B.V. undergoes an independent audit of its Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) practices. This audit, conducted annually, aims to evaluate the effectiveness and compliance of the company's AML/CTF/CPF program, ensuring it meets current legal standards and best practices to mitigate risks related to money laundering and terrorism financing.

Audit Objectives and Scope

The primary objective of the AML/CTF/CPF audit is to assess the company's adherence to the legal and regulatory requirements set by the Gaming Control Board and international

AML/CTF/CPF standards. The audit involves a comprehensive review of the company's AML/CTF/CPF program, including the following key areas:

- AML/CTF/CPF Policies and Procedures: Evaluating whether these policies are up-to-date and compliant with legal standards.
- Risk Management Assessment: Reviewing the effectiveness of the company's risk assessments and mitigation strategies.
- Transaction Monitoring Review: Assessing the efficiency of systems designed to detect and report suspicious activities.
- Staff Training Evaluation: Ensuring employee training programs are adequate and effective.
- Reporting Mechanism Audit: Examining the procedures for reporting suspicious transactions and compliance issues.
- Customer File Review: Verifying compliance with Know Your Customer (KYC), Know Your Business (KYB), and Customer Due Diligence (CDD) protocols.

Independent Auditor Selection

Infusion Tech B.V. engages an external or internal auditor with the appropriate expertise and resources to carry out the AML/CTF/CPF audit. The auditor must be independent from the company's AML Compliance team to avoid any conflicts of interest. The company carefully considers the auditor's credentials, experience, and reputation within the industry.

- The Gaming Control Board must approve the chosen auditor to ensure compliance with Curacao's gaming regulations.

Audit Process and Evaluation

The audit process follows both international standards and specific requirements set by the Gaming Control Board. Key steps include:

1. Evaluation of Policies and Procedures: Ensuring that the company's AML/CTF/CPF policies are updated and fully compliant with current legal requirements.
2. Risk Management Assessment: Reviewing how risks are identified and mitigated, and ensuring effective risk management strategies are in place.
3. Transaction Monitoring Review: Assessing the effectiveness of systems used to detect suspicious transactions and ensuring proper reporting.
4. Staff Training Evaluation: Verifying that training programs meet regulatory standards and that employees are properly equipped to detect and report suspicious activities.
5. Reporting Mechanism Audit: Checking how suspicious transactions and compliance issues are reported, ensuring that all processes are streamlined and accurate.
6. Customer File Review: Auditing the KYC, KYB, and CDD protocols to ensure that customer identification and risk assessment procedures are followed.

Audit Report and Findings

After the audit, the independent auditor provides a detailed report to the company's senior management and the Gaming Control Board. This report outlines the findings, recommendations, and any issues identified during the audit. Infusion Tech B.V. will act on the auditor's recommendations, implementing corrective actions within an established timeframe.

Gaming Control Board's Role

The Gaming Control Board, which oversees AML/CTF/CPF compliance for all licensed operators, reviews the audit results to ensure that the company is in full compliance. The Board may:

- Review the Audit Report: Analyzing the auditor's findings to assess compliance and highlight any concerns.
- Conduct Onsite Inspections: Verifying audit findings through visits to the company's premises to evaluate the effectiveness of corrective actions.
- Perform Interviews and Documentation Analysis: Interviewing relevant staff and reviewing supporting documents to better understand the company's AML/CTF/CPF practices.

Consequences of Non-Compliance

If the company is found non-compliant based on the audit or the Board's examination, penalties may include fines, operational restrictions, or suspension or revocation of the gaming license. Infusion Tech B.V. is committed to working closely with the Gaming Control Board to resolve any issues and maintain compliance to avoid such consequences.

14. RECORD KEEPING

The company adheres to rigorous record-keeping practices to ensure compliance with AML/CTF/CPF regulations. We prioritize maintaining secure, accurate, and accessible documentation to support regulatory compliance, internal audits, and the integrity of the gaming industry.

To meet legal requirements, the company retains key documentation for a minimum of five years. These records include all customer identification details collected during the onboarding process, transaction data, suspicious activity reports (SARs) submitted to the

Financial Intelligence Unit (FIU), training records for employees, and audit logs. These documents are critical for demonstrating compliance with the company's AML/CTF/CPF procedures and for assisting in any potential regulatory review or investigation.

All records are safeguarded through robust security measures. Encryption is employed to protect sensitive data, both when stored and during transmission. Access to records is restricted through strict controls, ensuring that only authorized personnel can access sensitive information. This access control system is regularly reviewed to ensure it aligns with the company's internal policies. In addition, the company conducts regular security audits to identify any vulnerabilities and confirm that the data remains secure and uncompromised.

To facilitate efficient retrieval, the company organizes all records systematically. Documents are stored in a secure, digital filing system that allows authorized personnel and regulatory bodies to quickly access the necessary information. This organizational structure ensures that records are easy to locate and review, especially during audits or inspections by regulatory authorities.

The company performs continuous internal monitoring and periodic audits to verify that record-keeping practices are in line with regulatory requirements. These audits assess the accuracy, completeness, and compliance of the records, ensuring that the company maintains high standards of data management. Additionally, the company supports regular reviews by regulatory bodies, ensuring that all records are properly maintained and available for examination.

The careful management of records is not only essential for meeting legal requirements but also plays a vital role in supporting the auditing and regulatory review process. Organized and secure record-keeping helps ensure that the company remains transparent and compliant with industry standards, contributing to the overall integrity of the gaming sector.

15. DEFINITIONS

Core Regulatory Concepts

- **AML (Anti-Money Laundering)** – Framework of laws, controls, and procedures to detect and prevent money laundering.

- **CTF (Counter-Terrorism Financing)** – Measures to detect, monitor, and prevent financial support for terrorist activity.
- **CPF (Counter-Proliferation Financing)** – Strategies to restrict the funding of weapons of mass destruction and related programs.
- **RBA (Risk-Based Approach)** – A methodology to assess and apply controls proportionate to the risk of financial crime.
- **Sanctions** – Legal prohibitions imposed on specific individuals, entities, or jurisdictions linked to criminal or geopolitical concerns.
- **Economic Sanctions** – Financial restrictions used to block access to the global financial system for sanctioned parties.

Customer Verification & Risk Assessment

- **KYC (Know Your Customer)** – The process of identifying and verifying the identity of clients.
- **KYB (Know Your Business)** – Verification of corporate entities, their ownership, and legitimacy.
- **CDD (Customer Due Diligence)** – Standard procedures to assess customer identity, behavior, and risk.
- **EDD (Enhanced Due Diligence)** – Additional verification measures for high-risk customers or complex transactions.
- **SDD (Simplified Due Diligence)** – Streamlined checks applied to low-risk customers under specific conditions.
- **PEP (Politically Exposed Person)** – A public figure subject to additional scrutiny due to corruption risk.
- **UBO (Ultimate Beneficial Owner)** – The individual with effective control over an account or business.
- **SOF/SOW (Source of Funds/Source of Wealth)** – Documentation of how a customer's funds are generated or accumulated.

Transaction Monitoring & Reporting

- **STR/SAR (Suspicious Transaction/Activity Report)** – A formal report submitted to the FIU when suspicious financial activity is detected.
- **Transaction Monitoring** – Ongoing review of transactions to identify unusual or high-risk patterns.
- **Unusual Transaction** – A transaction inconsistent with the expected behavior or financial profile of the customer.
- **Structuring** – A money laundering tactic involving fragmented transactions to evade detection.
- **Layering** – The complex movement of funds to obscure their criminal origin.
- **Integration** – The phase where illicit funds are introduced into the legitimate financial system.
- **Sanctions Evasion** – Attempts to circumvent financial or trade restrictions through deceptive means.

Oversight & Controls

- **Compliance Officer** – The person responsible for managing financial crime risk and maintaining independence from operational departments.
- **MLRO (Money Laundering Reporting Officer)** – A senior compliance official responsible for overseeing AML frameworks and reporting obligations.
- **BoD (Board of Directors)** – The corporate body accountable for ensuring AML program oversight.
- **First Line of Defense** – Employees responsible for implementing KYC/CDD and detecting red flags during onboarding or customer interactions.
- **Senior Management Oversight** – Executive accountability for the integrity of the AML/CTF framework.

Regulatory Bodies & Legal Instruments

- **FIU (Financial Intelligence Unit Curaçao)** – The national body responsible for reviewing and escalating suspicious activity reports.
- **FATF (Financial Action Task Force)** – A global authority on AML/CTF standards and enforcement.
- **CFATF (Caribbean Financial Action Task Force)** – A regional AML/CTF oversight group for the Caribbean and Latin America.
- **GCB (Curaçao Gaming Control Board)** – Regulatory authority for AML/CTF compliance in Curaçao's iGaming sector.
- **NOOGH (National Ordinance on Offshore Games of Hazard)** – Curaçao's legal framework governing online gaming.
- **OFAC (Office of Foreign Assets Control)** – U.S. agency administering economic sanctions and publishing the SDN list.
- **Egmont Group of FIUs** – An international network that fosters AML/CTF intelligence sharing and cooperation.
- **European Union (EU), United Kingdom (UK), United States (US)** – Key jurisdictions with binding AML/CTF legislation and enforcement mechanisms.

Risk Management Infrastructure

- **Blacklist** – A restricted list of individuals, businesses, or nations subject to sanctions or financial controls.
- **High-Risk Third Country** – Jurisdictions identified by FATF or the EU as lacking effective AML/CTF frameworks.
- **Comprehensive Sanctions** – Complete bans on dealings with certain jurisdictions or individuals.
- **AST (Automated Screening Tools)** – Software used to flag high-risk customers and transactions.
- **Real-Time Risk Assessment** – Immediate evaluation of transactions against defined risk criteria.

- **Internal Control Mechanisms** – Policies and procedures that mitigate AML/CTF risks.
- **Audit Logs** – Records of compliance actions retained for five years for regulatory inspection.
- **Corrective Action Plans** – Targeted compliance strategies implemented after audits or enforcement reviews.

Reporting & Governance

- **Customer File Review** – Periodic checks of client records for KYC/CDD completeness.
- **Reporting Mechanism Audit** – Verification that STRs and internal reports meet legal and procedural requirements.
- **Confidentiality in Reporting** – A legal mandate prohibiting unauthorized disclosure of SAR-related information.
- **Training and Awareness Programs** – Employee education on AML/CTF obligations and risk detection techniques.
- **Ongoing Monitoring** – Continuous surveillance of customer activity and risk profiles.
- **Regulatory Reviews** – External evaluations by supervisory bodies to ensure AML compliance.
- **Periodic Independent Audits** – Third-party assessments of AML/CTF program effectiveness.
- **Operational Restrictions** – Regulatory sanctions including suspension of licenses or monetary penalties for non-compliance.
- **Risk Appetite** – The level of risk an organization is willing to tolerate within its AML compliance structure.
- **Financial Crime Prevention Framework** – The overarching system of controls, assessments, and reporting that safeguards the organization from criminal exploitation.