

GAMMIX STS B.V.

Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) Policy

Disclaimer

NO PART OF THIS DOCUMENT MAY BE REPRODUCED, TRANSMITTED OR IN ANY OTHER WAY DISTRIBUTED WITHOUT THE PRIOR WRITTEN PERMISSION OF GAMMIX STS B.V. ALL TECHNOLOGIES, DESIGNS, IMPLEMENTATIONS, TRADE SECRETS AND BUSINESS MODELS DESCRIBED HEREIN IS THE INTELLECTUAL PROPERTY OF GAMMIX STS B.V., AND/OR IT'S PARTNERS AND IS PROVIDED FOR INFORMATION PURPOSES ONLY.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY CONCERNING ITS ACCURACY OR QUALITY. IN NO EVENT WILL GAMMIX STS B.V. BE LIABLE FOR DIRECT OR INDIRECT DAMAGES RESULTING FROM INCIDENTAL DEFECTS OR INACCURACIES IN THIS DOCUMENT.

GAMMIX STS B.V. RESERVES THE RIGHT TO REVIEW AND MODIFY DIGITAL COPIES OF THIS DOCUMENT AT ANY TIME WITHOUT PRIOR NOTICE.

THE GAMMIX STS B.V. NAME, THE GAMMIX STS B.V. LOGOTYPE, GAME BRANDS, SERVICES AND PRODUCT NAMES ARE REGISTERED TRADEMARKS AND/OR SERVICE MARKS OF GAMMIX STS B.V.

Contact

GAMMIX STS B.V.
Mark Cauchi
+356 2166 0939
compliance@kmlpartners.com

Document Version Control

GAMMIX STS B.V. – AML/CTF Policy	
VERSION CONTROL	
Current version	1.1
Effective Date	25/04/2025
Sign Off Date	25/04/2025
Document Owner	Senior Compliance Officer / MLRO
Next Review Date	24/04/2026
Comments	The policy will be reviewed on the following basis: No less than once annually, with such review to be initiated by the Policy owner approximately one month prior to the date following 12 months from which the procedure was last approved. · In response to any changes in relevant regulation and/ or legislation. · In response to general guidance notes or best practice guidance issued by any relevant regulator. · In response to any regulatory action taken · In response to findings of a relevant internal or external audit; or · Upon request of management.
Purpose	Creation of this AML/CTF Policy

Version history

Version	Date	Author	Purpose
1.0	10/02/2025	Gammix STS B.V.	Creation of this document
1.1	25/04/2025	Gammix STS B.V.	Policy update to reflect regulatory changes published by CGA (AML/CTF Policy Template)

Table of Contents

1. Introduction & Background	7
1.1 Scope & Purpose	7
1.2 Regulatory framework	7
1.3 Applicable definitions	7
1.3.1 Money Laundering	8
1.3.2 Terrorist financing	8
1.3.3 Financing of Proliferation of weapons	8
1.4 Client and Applicant for Business	8
1.5 Audience	9
1.6 Laws, Regulations and Rules	9
1.7 Consequences of non-compliance	9
2. Document structure	10
3. AML Systems and Controls – General	11
3.1 Policy	11
3.2 Procedures and documentation	12
4 Risk Assessment, Management and Risk-Based Approach	13
4.1 Guidance on Implementation of Risk-Assessment Procedures	13
4.2 Business Risk Assessment	14
4.2.1 Risk Categories Assessed	14
4.2.2 Overall Risk Assessment Summary	16
4.2.3 Risk Management Approach	16
4.2.4 Review and Update	16
4.3 Policy	16
4.4 Procedures & Documentation	18
4.5 Client transactions	19
4.5.1 Amount of funds being transacted	19
4.5.2 Nature and frequency of transactions	19
4.5.3 Ongoing monitoring of transactions	20
5 Client Due Diligence	20
5.1 Policy	20
5.2 Procedures and Documentation	21
5.3 Client Due Diligence (CDD) Procedure	21
5.4 Identification & Verification	21
5.5 Enhanced Partner due diligence	22
6. Ongoing monitoring	22
6.1 Policy	22
6.2 Procedures and Documentation	23

7. Reporting	23
7.1 External Reporting	23
7.2 Suspicious Activity Reporting	23
7.3 Guidance on Implementation	24
7.4 Policy	25
7.5 Procedures and Documentation	26
8 Record-Keeping Procedures	27
8.1 Guidance on Implementation	27
8.2 Policy	27
8.3 Procedures & Documentation	28
9. Awareness and Training	28
9.1 Guidance on Implementation	28
9.2 Policy	29
9.3 Procedures & Documentation	30
9.4 Anti-Bribery & Corruption Policy	31
11. Sanctions Lists	32
11.1 Guidance on Implementation	32
11.2 Policy	33
11.3 Procedures and Documentation	33
12. Politically Exposed Persons	34
12.1 Guidance on Implementation	34
12.2 Policy	34
12.3 Procedures and Documentation	35
Annex I – Senior Compliance Officer / MLRO Job Description	36
Annex II – Risk Mitigation Matrix and Risk Factors	38
Risk Assessment and Mitigation Matrix	38
Risk Factors Table	38
Process for Determining Client Risk	38
Annex III – Client Due Diligence	39
Persons subject to Identification and Verification	39
Due Diligence for Natural Persons	40
Due Diligence for Legal Persons	41
Part A	41
Part B	43
Part C	43
Languages	43
Client Terms and Conditions	44
Client Risk Assessment	44

Face-To-Face Transactions or Clients 44

Timing of Due Diligence..... 44

Annex IV – Client Acceptance Policy 45

Client Acceptance 45

Excluded Activities..... 45

Excluded Individuals 45

Risk-Based Approach for Accepting Clients..... 46

Annex V – Internal STR/SAR Form 47

Annex VI – Abbreviations..... 49

Annex VII – Signatory page 50

Curaçao

1. Introduction & Background

1.1 Scope & Purpose

The Anti-Money Laundering Policy (“AML Policy”) and the procedures outlined within apply to Gammix STS B.V. (“Gammix STS” or the “Company”).

The provisions of this Policy aim to reduce the possibility for the business and associated providers to be used for criminal purposes or violate the applicable regulations and therefore adhere to the requirements. This Policy covers the following key risk areas:

- Anti-Money Laundering (“AML”);
- Sanctions; and,
- Politically Exposed Persons (“PEPs”).

Defined as a Games Aggregator, Gammix STS B.V. is deemed to be carrying out “relevant financial business” in terms of the Prevention of Money Laundering and Funding of Terrorism and as such, the Company is a subject to various Regulations. Therefore, Gammix STS B.V. is required to abide by the applicable legislation and guidance relating to the prevention of Money Laundering (“ML”) and Terrorist Financing (“TF”).

This Policy provides guidance detailing Gammix STS B.V.’s responsibility to prevent ML and outlines the compliance framework implemented in order to do so. The framework takes into consideration the relevant applicable regulations, in addition to industry best practices. This Policy includes (but is not limited to):

- Due Diligence;
- Ongoing monitoring;
- Training;
- Record-keeping; and,
- Roles and responsibilities of the Money Laundering Reporting Officer (“MLRO”).

1.2 Regulatory framework

Outlined below is a list of all relevant AML legislation, regulation, and codes that this Policy has been written in accordance with:

- The relevant Regulations Concerning Anti-Money Laundering and Counter Terrorism Financing (the “Regulations”);
- International standards and recommendations as outlined by the Financial Action Task Force (“FATF”).

1.3 Applicable definitions

1.3.1 Money Laundering

“Money laundering” means:

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement;
- Layering; and
- Integration.

1.3.2 Terrorist financing

“Terrorist financing” or “Financing of Terrorism” means:

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

1.3.3 Financing of Proliferation of weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

1.4 Client and Applicant for Business

The direct client of Gammix STS B.V. and applicant for business shall be the partner (or client) who enters into an agreement with the Company - or with a group company which who a service agreement is in place.

A **Client** refers to an operator, casino, or betting platform that has an established business relationship with the game aggregator. The client integrates the aggregator’s portfolio of games into their platform, enabling them to offer a variety of gaming content (slots, table games, live dealer, etc.) to their end users. Clients may also receive additional services such as API support, backend management, and regulatory compliance assistance.

An **Applicant** is a prospective operator, casino, or platform that is in the process of applying to partner with the payment processor. This entity has expressed interest in integrating the aggregator’s games but has not yet completed the onboarding or approval process. The applicant will be undergoing due diligence, compliance checks, or technical assessments before becoming a full-fledged client.

1.5 Audience

This AML Policy applies to all employees, officers, directors, contractors, consultants, and any other individuals or entities acting on behalf of the Company, regardless of location or job function.

It is particularly relevant for individuals engaged in the following activities:

- Customer onboarding and due diligence
- Financial transactions and payment processing
- Compliance and risk management
- Legal and regulatory affairs Internal audit and controls
- Sales and account management

All personnel must understand their responsibilities under this policy and complete any required AML training provided by the Company. Failure to comply with the obligations outlined in this policy may result in disciplinary action, up to and including termination of employment or contract.

Third-party partners, agents, and service providers who represent or act on behalf of Gammix STS B.V. may also be required to comply with this policy, as determined by the nature of their relationship with the company.

1.6 Laws, Regulations and Rules

The Code of Criminal Law (Penal Code) of Curaçao lays down the procedures for the prosecution of a money laundering offence, as well as the measures for the confiscation of property upon a conviction of money laundering, measures for the freezing of assets when a person is charged with an offence of money laundering and measures for the issuance of an investigation and/or attachment order when a person is suspected of having committed an offence of money laundering.

The policies and procedures in this Policy aim to comply with both the rules and guidance contained in the NOPML, the NORUT and the NOIS which regulations themselves are referring to the Penal Code. In addition to these regulations the Curaçao Gaming Authority has introduced a comprehensive framework with provisions and guidelines to prevent and combat money laundering and terrorist financing. Curaçao - as a member of the FATF - has based these guidelines on, among others, the FATF recommendations.

1.7 Consequences of non-compliance

Violations of this AML Policy can expose the Company, its employees, and its partners to significant legal, regulatory, and reputational risks. Understanding and complying with this policy is essential to protect the integrity of our operations and to fulfill our legal and ethical obligations.

Disciplinary actions

Any employee who fails to comply with this policy may be subject to disciplinary action, which may include:

- Formal warnings;
- Suspension;
- Termination of employment or contract;
- Loss of professional licenses or certifications.

Contractors or third parties found in violation may face termination of agreements and disqualification from future business with Gammix STS.

Legal implications

Non-compliance with AML regulations can result in severe legal consequences, including:

- Civil or criminal prosecution;
- Substantial fines and financial penalties;
- Imprisonment of individuals involved;
- Asset seizures or freezing of funds;
- Disqualification from serving as a company officer or director.

Business and reputational risks

Violations can also damage the company's reputation, investor confidence, and customer trust. Potential consequences include:

- Regulatory investigations or sanctions;
- Loss of partner relationships;
- Increased scrutiny from financial authorities;
- Negative media exposure and reputational harm;
- Financial loss due to operational disruptions or terminated business relationships.

2. Document structure

Each section below is divided into the following parts:

- a) Guidance on implementation (where applicable);
- b) Gammix STS B.V.'s policy; and,
- c) Procedures and Documentation – the processes by which the policy referred to is (or will be) implemented, including reference to other documents as appropriate.

3. AML Systems and Controls – General

Due Diligence should be applied:

- i) When establishing business relations;
- ii) Where there is a suspicion of ML or TF;
- iii) Where there is doubt about the veracity or adequacy of previously obtained identification data.

The Company is obliged to apply the above measures and procedures including the cases when entering into or undertaking non-face-to-face relationships or transactions directly or indirectly.

The Company is also obliged to establish policies and procedures on risk management practices, internal controls, record keeping, and the monitoring and management of compliance with the aforesaid policies, controls and procedures to adequately and appropriately mitigate risk and prevent the carrying out of operations that may be related to money laundering or the funding of terrorism.

The Company must ensure that employees are made aware of applicable AML/CFT legislation as well as the Company's policies and measures in this regard. Employees of the Company must undergo appropriate due diligence procedures prior to their engagement, when transferred or when promoted. Employees are also expected to be provided with training regarding the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

3.1 Policy

Responsibility

The ultimate responsibility for the AML Policy of Gammix STS B.V. is with the Senior Compliance Officer/MLRO. Day-to-day responsibility for the development and implementation of policies and procedures contained within this Policy is delegated to the Senior Compliance Officer/MLRO.

AML Policies and Procedures

The policies and procedures operated by Gammix STS B.V. in order to meet applicable AML regulations, including relevant AML and CFT requirements are documented in this Policy. Policies and procedures will be regularly reviewed to ensure that they continue to meet regulatory requirements and the changing risk environment as per Gammix STS B.V. as far as applicable.

AML Risk

The Senior Compliance Officer / MLRO will undertake regular assessments of the ML risks and Gammix STS B.V.'s strategy and success in mitigating those risks. Gammix STS B.V. will document its risk management policies and risk profile in relation to AML, including its application of such policies and in subsidiary documentation referenced herein.

The Company uses the following guidance as a base for its AML risk model:

- i. A clear statement of the culture and values adopted towards the prevention of financial crime;
- ii. A commitment to ensuring that identity will be satisfactorily verified in all cases and in a risk-based manner, before applicants for business are accepted as clients;
- iii. A commitment to ongoing due diligence throughout the business relationship;
- iv. A commitment to ensuring that staff are trained and aware of the law, their legal obligations, and how to meet those obligations; and,
- v. A clear allocation of roles, responsibilities and organizational structure, and recognition of the importance of staff promptly reporting their suspicions internally.

3.2 Procedures and documentation**Responsibility**

The delegated day-to-day responsibility for the AML policy and operation of effective procedures is documented in the Senior Compliance Officer's / MLRO's Job Description in Annex I below.

Responsibility for the review and update of the AML Policy, and applicable sections, additionally rests with the Senior Compliance Officer / MLRO. Each version of the AML Policy will be reviewed and approved by the Board of the Company prior to being issued and will carry a review and approval date.

AML policies and procedures

The AML Policy is subject to Gammix STS B.V.'s local policies and procedures regarding compliance monitoring, record keeping and reporting.

The AML Policy is reviewed periodically and, as necessary, updated in order to reflect changes in legislation, national and international findings, the profile of Gammix STS B.V.'s client base, and the services offered.

The procedures detailed within this Policy do not just reflect the AML obligations of the Company, but consider the regulatory requirements imposed any relevant Regulator and suggested within the FATF Recommendations. This Policy must be adhered to by all Company staff, including companies belonging to Gammix STS B.V.

AML risk factors

An AML partner risk assessment overview will be maintained in order to allocate and track the

components of the separate risk classifications. Gammix STS B.V. categorizes overall AML risk based on the below risks of the Client:

- Strategic risk
- Financial risk
- Compliance risk
- Geographic risk
- Technical risk
- Subsequential risk
- Resource risk
- Replacement risk
- Operational risk
- Reputational risk
- Existence of PEPs
- Type of provision or service
- ML or TF risk of provision
- Monitoring process
- Negative screening result on adverse media
- Client's responsiveness to provide requested Due Diligence

4 Risk Assessment, Management and Risk-Based Approach

Gammix STS B.V. is required to have P&Ps in place to mitigate specific risks involved with business transactions or non- face-to-face transactions.

Based on the FATF recommendations, Gammix STS B.V. is allowed to apply an RBA. By adopting an RBA, it is possible for service providers such as Gammix STS B.V. to ensure that measures to prevent or mitigate ML and TF are commensurate with the risk identified. Although all clients are subject to minimum due diligence standards, clients identified as high risk must be subject to EDD, whilst low risk clients may be subject to the standard minimum client due diligence.

4.1 Guidance on Implementation of Risk-Assessment Procedures

Risk Assessment

For the implementation of risk-assessment procedures, the AML Regulations recognizes the FATF Standards and that the Company should prepare a risk-assessment, as well as policies, controls, and procedures curated to manage and mitigate ML/FT risks.

The purpose of the risk-assessment procedures is to enable the Company to be in a position to identify and assess the ML/TF risks that the Company is or may become exposed to and thereby determine:

- a) Whether the application of enhanced due diligence is necessary;

- b) The point in time when the application of CDD should be applied; and,
- c) Whether a client presents a low risk of ML/FT for the purposes of delaying the performance of verification proceedings to after the commencement of a business relationship, as has been discussed above.

Monitoring Controls

It is essential that the controls to manage and mitigate the identified risks are constantly monitored. This should be done so that in the event of a change in circumstances, which might mitigate or exacerbate a particular risk, the respective control is modified accordingly.

For instance, it is important that the Company has a system in place to identify changes in client's characteristics, as this would obviously have a bearing on the risk profile of the client. Similarly, the threat posed by a particular product or service may cease to exist, which would lead to a reconsideration of the risk scoring of the business relationship. In view of this, the Company must be in a position to identify such changes.

The Company should also carry out periodic internal audits or assessments to review the adequacy of the risk assessment, the internal controls and the compliance arrangements. Such audits or assessments should also review the effectiveness of liaison between the different departments of the organization, and the effectiveness of the balance between technology-based and people-based systems. The review should also consider the effectiveness and compliance of third parties used by Gammix STS B.V.

4.2 Business Risk Assessment

As part of Gammix STS's AML Policy, this Business Risk Assessment (BRA) is conducted to identify, assess, and mitigate the risks of money laundering and terrorist financing (ML/TF) to which the Company may be exposed. In accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT) and other applicable Curaçao regulatory requirements, Gammix STS maintains a risk-based approach to AML compliance.

The Company operates as a Games Aggregator, supplying games and software integration services to licensed B2C operators globally. Although the Company does not operate a consumer-facing platform or handle player funds directly, it acknowledges its critical role in the gaming ecosystem and the potential exposure to ML/TF risks through its clients and business relationships.

4.2.1 Risk Categories Assessed

4.2.1.1 Customer Risk (B2B Operators)

Risk factors:

- Operating jurisdictions (high-risk or non-cooperative countries);

- Strength of the customer's own AML controls and licensing status;
- Nature of games offered (e.g., high-risk games like virtual slot machines);
- Use of cryptocurrencies by B2C operators.

Mitigating measures:

- Onboarding only licensed and regulated B2C clients.
- Enhanced due diligence (EDD) on clients from high-risk jurisdictions.
- Ongoing client reviews and periodic reassessment of risk profiles.
- Requiring evidence of AML policies and technical integration standards.

4.2.1.2 Product/Service Risk

Risk factors:

- Aggregated game content may be used in B2C platforms without full transparency.
- Integration with third-party systems, including payment processors and wallet services.
- Limited visibility into end-user (player) activity.

Mitigating measures:

- Contractual clauses restricting sublicensing or resale without prior approval.
- Technical monitoring tools and analytics to detect unusual operator behavior.
- Review of game usage data for inconsistencies or suspicious trends.

4.2.1.3 Geographic Risk

Risk factors:

- Exposure to clients operating in high-risk or sanctioned regions.
- Potential indirect exposure through white-label or sublicensing arrangements.

Mitigating measures:

- Use of reliable third-party screening tools to assess jurisdictional risk.
- Refusal of business from sanctioned countries or unregulated operators.
- Periodic review of regulatory lists and sanctions regimes.

4.2.1.4 Delivery Channel Risk

Risk factors:

- Remote onboarding and automated integrations may reduce manual oversight.
- Limited physical presence or verification of certain counterparties.

Mitigating measures:

- Rigorous client onboarding procedures with document validation and beneficial

ownership checks.

- Verification of technical integration endpoints and IP restrictions.
- Use of secure APIs and controlled access to aggregation platforms.

4.2.2 Overall Risk Assessment Summary

Based on the above, Gammix STS categorizes its overall ML/TF risk exposure as **moderate**, with elevated risk primarily arising from:

- Clients operating in higher-risk jurisdictions.
- Limited visibility over downstream player activities.
- Potential misuse of aggregation services by non-compliant operators.

However, through robust onboarding, monitoring, and contractual enforcement mechanisms, these risks are managed to an **acceptable** level.

4.2.3 Risk Management Approach

Gammix STS adopts a risk-based approach to AML compliance, which includes:

- Conducting risk assessments at the onboarding stage and reviewing them annually or upon significant changes.
- Applying enhanced due diligence where higher risk is identified.
- Training relevant staff on ML/TF risks and red flags specific to the B2B gaming sector.
- Cooperating with regulators and Financial Intelligence Units (FIUs) in Curaçao and other relevant jurisdictions.

4.2.4 Review and Update

This Business Risk Assessment shall be reviewed at least annually, or more frequently where material changes in the business model, client base, or regulatory landscape occur.

4.3 Policy

Risk-Based Approach

Gammix STS B.V. operates a Risk-Based Approach (“RBA”) to develop and operate its systems and controls designed to prevent financial crime. AML risk is analyzed, as applicable, into the following risk categories:

- Strategic risk

- Financial risk
- Compliance risk
- Geographic risk
- Technical risk
- Subsequential risk
- Resource risk
- Replacement risk
- Operational risk
- Reputational risk
- Existence of PEPs
- Type of provision or service
- ML or TF risk of provision
- Monitoring process
- Negative screening result on adverse media
- Partner's responsiveness to provide requested DD

The Risk Assessment and Mitigation Matrix in Annex II to this Policy identifies and explains the risks inherent to the particular services provided by Gammix STS B.V., as well as the actions taken by the Company to mitigate these risks.

The Risk Factor table also in Annex II to this Policy identifies risk factors relevant to Gammix STS B.V.'s business that indicate a risk of money laundering or terrorist financing.

AML risk assessment

The Senior Compliance Officer / MLRO will perform regular assessments of the ML risks and Gammix STS B.V.'s strategy and success in mitigating those risks.

Where a new service or new geography is addressed by Gammix STS B.V., the AML risk assessment will be updated during development/launch (to ensure that AML processes can support the new activities). The results of the AML risk assessment will be used to support the development of appropriate systems and controls (policies and procedures) designed to minimize the risk of Gammix STS B.V., being used for the purposes of AML. All developments will be reported to the Board of Directors.

Risk Mitigation

In order to mitigate the risk of ML, Gammix STS B.V. will ensure that appropriate risk-based systems and controls are in place and operated for, amongst others, the Company as prescribed in Annex II below. Existing systems and controls will be reviewed and where necessary amended to reflect changes in assessed risk and identified vulnerabilities. Additional systems and controls will be implemented by the Senior Compliance Officer / MLRO where required.

Monitoring Controls

The AML Policy will be subject to Gammix STS B.V.'s policies and procedures regarding compliance monitoring. The Senior Compliance Officer / MLRO will ensure that the internal controls operated by Gammix STS B.V. are reviewed when there are changes to regulations or Gammix STS B.V.'s arrangements / products / markets.

When there is a change in Gammix STS B.V.'s AML policies or in the AML regulations, this Policy, and associated materials, will be updated and details of the changes included in the Senior Compliance Officer / MLRO's Annual Report.

4.4 Procedures & Documentation

Risk-Based Approach

The application of the RBA in the prevention of AML is reflected in Gammix STS B.V.'s approach to the operation and development of the systems and controls implemented and are designed to minimize the risk of Gammix STS B.V. from being used for the purposes of AML Risk is central to the development of the business, new products, development of product functionality or the operation in new markets. The RBA is referenced in all Gammix STS B.V. AML documentation.

AML Risk Assessment

AML risk assessments are undertaken on an ongoing basis, and in particular, applied when the business environment changes through, for example:

- Entry into new markets; and
- Development of new products or product features / functionality.

Risk mitigation activities, i.e. the development of appropriate internal controls, flow from the findings of the risk assessments.

Risk assessments and the development of mitigating actions are documented in Annex II below and are accordingly reported to the Board of the Company.

Risk Mitigation

Gammix STS B.V. seeks to minimize the opportunities for carrying out financial crime, i.e. money laundering or funding of terrorism, and to then address and mitigate any risks that remain as further set out in Annexes II and III below. Internal controls focus on:

- Due diligence of Clients, including levels of enhanced due diligence ("EDD") based on risk assessments of each Client;
- Assessing risks and setting out measures to mitigate the said risks;
- Monitoring key risk factors for reassessing a specific Client's risk; and
- AML systems and controls will continue to be developed over time in order to adequately address the changing risk environment.

Monitoring Controls

This Policy is reviewed and, if necessary, updated continuously in order to reflect changes in the AML policies and procedures which affect the operations of Gammix STS B.V. Consequently, the Senior Compliance Officer / MLRO's regularly reviews the following areas:

- a) Developments in legislation, including the AML Regulations; and the AML Policy.
- b) The AML risk assessments – whose performed as part of the development of new products, services, functionality or addressing new Clients / markets.
- c) The operation of periodic internal controls, including monitoring, investigation, and reporting of suspicious activity.
- d) New typologies for fraud or AML, including feedback from regulators or law enforcement.
- e) Feedback received following the provision of training or Compliance reports to the Board by the Senior Compliance Officer / MLRO.

Document	Title	Frequency	Audience	Responsibility
Report	MLRO Internal Audit Report	Annual	Board	Senior Compliance Officer / MLRO

4.5 Client transactions

4.5.1 Amount of funds being transacted

The Company assesses the expected level of business at the outset of the relationship and reviews on an ongoing basis. If funds transacted are outside of the expected level, there is an enhanced risk of money laundering or terrorist financing activities and additional checks will be undertaken. On its own, the risk associated with large transactions may not be overly significant. However, when combined with irregular or unusual activity or with the PEP status or location of the partner, the risk may be significantly increased.

4.5.2 Nature and frequency of transactions

Where a partner is making regular transactions within the expected parameters there is considered only minimal potential risk of money laundering or terrorist financing. Irregular patterns of activity or regular transactions may highlight enhanced risk. The procedures detailed in the following pages address both the requirement to identify partners and to gather evidence verifying the Directors / UBOs identity, but also to monitor on-going activity to determine a change in the risk profile of the partner.

4.5.3 Ongoing monitoring of transactions

All transactions by all partners are recorded and can be reported on an ad-hoc basis for monitoring purposes.

It is recognized that a significant change to the normal operation of a partner could be a sign of suspicious activity.

A change may be:

- Unusually large transactions based on past account history; and
- Multiple changes to the business address details.

In addition, changes made to the partner's identity and personal information will be reported on to the Company's management. The evidence of identity previously provided by the partner will be reviewed and steps taken to renew and update that information in light of the reported changes to the partner's identity. In certain cases, this may mean that the account is suspended pending receipt of new identity and address verification.

In the event that satisfactory confirmation of the information as to the identity of the partner or satisfactory verification of evidence of identity is not provided, then the onboarding will be stopped, no further trading allowed, and consideration be given to the lodging of a suspicious transaction report.

5 Client Due Diligence

Due Diligence measures are to be applied in the following cases:

- When establishing business relationships;
- When carrying out occasional business transactions;
- When the Company suspects that a transaction may involve ML/FT; or
- When the Company doubts the veracity or adequacy of previously obtained identification data, for the purpose of identification or verification.

5.1 Policy

Clients of the Company are subject to risk-based initial and ongoing due diligence procedures according to the risk categories outlined in Annex II below and the Client due diligence procedures set out in Annex III below.

Initial due diligence seeks to obtain the identity of the Directors / UBOs and verify the identity prior to the establishment of the business relationship. Ongoing monitoring procedures ensure that the initial due diligence information remains up to date.

5.2 Procedures and Documentation

The detailed procedures for the performance of risk-based client due diligence are detailed in section 5.3 and 5.4 and also in Annex III below relating to Client Due Diligence and Enhanced Due Diligence.

Document	Title	Frequency	Audience	Responsibility
AML Policy, Annex II	Risk Mitigation Matrix and Risk Factors	As required	Relevant staff	Senior Compliance Officer / MLRO
AML Policy, Annex III	Client Due Diligence	As required	Relevant staff	Senior Compliance Officer / MLRO
AML Policy, Annex IV	Client Acceptance Policy	As required	Relevant staff	Senior Compliance Officer / MLRO

5.3 Client Due Diligence (CDD) Procedure

CDD standards are designed to protect the Company against fraud, corruption, money laundering and terrorist financing. CDD is a verification check carried out by the Company to:

- Identify that the Client / Director / UBO is who they say they are;
- Verify that the Client / Director / UBO is over 18;
- Combat and reduce fraud;
- Prevent money laundering; and
- Confirm that the funds being used in during the business relationship are genuinely the Client's.

5.4 Identification & Verification

Before a Client (Business Partner) is onboarded, the following information / documentation is required.

- Certificate of incorporation and registration
- Memorandum & Articles of Association
- Structure chart
- Copy of gambling licenses / permits
- Register of Directors & Members

- Certified Copy of Director(s) Passport(s)
- Certified Copy of Director(s) Proof of Address(es)
- Certified Copy of UBO's Passport(s) - 25% + 1% or above
- Certified Copy of UBO's Proof of Address(es) - 25% + 1% or above
- Declaration of trust (where applicable)
- Client's CDD/AML Policy
- Any other relevant policy / procedure listed by the business

5.5 Enhanced Partner due diligence

In certain cases, highlighted by the risk assessment, Senior Management may consider that a partner poses a higher risk. In these circumstances, EDD will be requested and collected by the Company. Partners who pose an additional risk will be marked within the system and a report of their transactions made available to the MLRO.

6. Ongoing monitoring

The Company must implement ongoing monitoring for the duration of the business relationship and not just at the initial onboarding stage. Ongoing monitoring must include (but is not limited to):

- Regular screening against PEP, sanctions, and adverse media databases.
- Transaction Monitoring activities. Client must be monitored and compared to the applicable expected Client transactional profiles. Unusual activity must be investigated and, in the case of potentially suspicious activity / transaction, will be escalated to the Senior Compliance Officer / MLRO in the form of a Suspicious Activity Report.

6.1 Policy

Ongoing monitoring processes will focus on ensuring that due diligence information provided is up to date and that no documentation is expired. On-going monitoring will also ensure that there have been no material changes to the Client that affects the risk profile of the Client.

On-Going Monitoring Measures

On-Going Monitoring will be conducted on a continual basis for all Clients and applicable Third Parties. On-Going Monitoring will include:

- Ongoing Screening: Daily/Weekly screening against all relevant sanctions, PEPs, and adverse media lists.
- Periodic Review: Periodic Reviews will be commensurate to the ML/TF risk associated with the Client.
- Event Driven Reviews ("EDR"): An EDR will be initiated on the identification of a high-risk factor or red flag during the ongoing monitoring process (including Transaction Monitoring).

Due Diligence information

Due diligence information will be reviewed as follows to ensure that it remains up to date.

Low Risk Clients: Once every 2 years

Medium Risk Clients: Annually

High Risk Clients: Quarterly

6.2 Procedures and Documentation

The Company notes that it offers a single service to its Clients whereby the applicant for business is affecting payments for game aggregator services. Therefore, in all cases, the Company understands the nature of the relationship with the Client and all payments received are sourced from this business.

Training will be provided to relevant staff to ensure that they are aware of the requirement to stay alert to the possibility of suspicious activity and what suspicious activity might comprise. Training is addressed in Section 9 below.

Client due diligence information set out in Annex III will be periodically reviewed to ensure that it remains up to date as per the above. This review is recorded by way of assessing whether any due diligence information has expired.

The review will also assess whether any changes have been made to the company structure and/or the people involved. In such an instance, due diligence will be updated accordingly.

7. Reporting

7.1 External Reporting

The Company have an obligation to report to the FIU, or Direct Licensee on behalf of the FIU, on any identified instances of suspicious activity where the Company knows of or reasonably suspects that certain behavior on the part of the Client may be related to money laundering activity or where such activity appears to be unusual or at variance with the usual behavior or transactional activity of the Client. The Company must share all Suspicious Activity Reports with the FIU; and/or may be required to report on request, to the FIU, or Direct Licensee on behalf of the FIU, on additional AML/CFT requirements as deemed appropriate.

7.2 Suspicious Activity Reporting

The Company must lodge a suspicious activity report if, at a particular time:

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

A suspicious activity report concerning a possible money laundering offence or other criminal offence must be lodged with the FIU promptly after the day on which the reporting entity forms the relevant suspicion.

A suspicious activity report concerning or in relation to possible financing of terrorism, must be lodged within 24 hours after the time when the Company forms the relevant suspicion.

A suspicious activity report must contain a statement of the grounds on which the Company holds the relevant suspicion.

A reporting entity shall fully document the reasons for any decision regarding the submission or non-submission of a suspicious matter report.

7.2.1 *Tipping off*

If a reporting entity forms:

- a) A reasonable suspicion;
- b) Lodges a suspicious activity report with the FIU; or,
- c) provides documents or other information to the FIU;

neither the reporting entity nor any person employed or associated with the entity may disclose to someone other than the FIU that the suspicion has been formed, report lodged, or information has been communicated to the FIU, as applicable.

7.3 Guidance on Implementation

Internal Reporting

If the Senior Compliance Officer / MLRO concludes, for justifiable reasons, that an internal report does not give rise to a suspicion, the Senior Compliance Officer / MLRO need not inform the FIU. In this case, the MLRO shall keep a written record of the internal reports received, the assessment conducted, the outcome and the reasons why the report was not submitted to the FIU. Upon request by the FIU or the relevant supervisory authority acting on behalf of the FIU, or in completing the Annual Compliance Report, the Senior Compliance Officer / MLRO will make such information available.

7.4 Policy

Annual Compliance Report and MLRO Report

The Senior Compliance Officer / MLRO shall also prepare an “MLRO Report” to be presented to the Directors to outline issues pertinent to the management of financial crime, of which the Board should be aware. This MLRO Report is for internal purposes and does not need to be submitted to the Regulator.

Internal Reporting

Gammix STS B.V.’s reporting policy applies to the ‘relevant staff’ of Gammix STS B.V., Providers and Distributors. Relevant staff are those that handle or who are managerially responsible for handling, or are otherwise ‘close’, to Client transactions or accounts (Consumers and Merchants).

Gammix STS B.V. will generate two types of suspicious activity reports:

- **Internal STRs** - Internal suspicious activity reports may be generated by all relevant staff. Internal STRs are used to report suspicious activity to the Senior Compliance Officer / MLRO, and
- **External STRs** - External suspicious activity reports are produced by the Senior Compliance Officer / MLRO in the event of suspicious activity having been identified and confirmed through investigation. External STRs are submitted to the FIU.

Records relating to both Internal and External STRs are kept in accordance with Gammix STS B.V.’s record-keeping policy. Internal and external STRs are kept for a minimum period of 5 years.

All relevant staff will receive both initial and ongoing training on anti-money laundering, detection of suspicious activity and the internal reporting process.

Internal Reporting – Gammix STS B.V. Staff

Where a Gammix STS B.V. employee knows or suspects, or has reasonable grounds for knowing or suspecting, that any Client is engaged in money laundering, they must report these suspicions to the Senior Compliance Officer / MLRO using the Internal STR/SAR Form (please find it in Annex V).

Any Gammix STS B.V. staff member that does not adhere to the internal reporting requirements will be subject to disciplinary process.

Internal Reporting – Providers and Distributors

Where any relevant staff member in a Provider or Distributor, knows or suspects, or has reasonable grounds for knowing or suspecting, that any Client is engaged in money laundering, they should report their suspicion directly to the Gammix STS B.V.’s Senior Compliance Officer / MLRO.

External Reporting (Senior Compliance Officer / MLRO)

Where a suspicious activity report has been made to the Senior Compliance Officer / MLRO he/she will conduct investigations and access information on the Client, or the transaction, as necessary.

Where appropriate, an STR/SAR will be made to the FIU by the Senior Compliance Officer / MLRO which will include the mandatory information regarding the Client's account and the transaction(s) involved.

7.5 Procedures and Documentation**Senior Compliance Officer / MLRO Role**

The responsibilities associated with the Senior Compliance Officer / MLRO role are documented in the Senior Compliance Officer / MLRO Job description.

To ensure that Gammix STS B.V. maintains an AML approach that meets regulatory requirements, the Senior Compliance Officer / MLRO will regularly review developments in legislation and their impact on the policies and procedures contained in this Policy, including:

1. National and International Findings; and
2. Local legislation in the countries of relevant Providers and Distributors.

If changes in the relevant anti-money laundering legislation are found to contribute to an increased risk of money laundering, through the periodic performance of an AML risk assessment, the policies and procedures in this AML Policy will be updated by the Senior Compliance Officer / MLRO. The Senior Compliance Officer / MLRO communicates changes in policies and procedures to all relevant parties.

In order to ensure that Gammix STS B.V. AML approach addresses current AML risk, the Senior Compliance Officer / MLRO undertakes regular financial crime risk assessments and considers the Gammix STS B.V. strategy and success in mitigating those risks, using the risk categories detailed in Annex II. The performance of risk assessments is detailed in Section 3 above. The results of these periodic assessments will be regularly reported to the Board of the Company.

Internal Reporting

Relevant staff will receive initial and periodic training to ensure that their reporting obligations, and the method of making an Internal STR, are understood as well as to assist them to recognize suspicious activity. Typologies are maintained and will be used as part of the training provided.

Internal STRs should be sent to the Senior Compliance Officer / MLRO using the 'Gammix STS B.V. Internal STR/SAR Form'. The Senior Compliance Officer / MLRO acknowledges the receipt

of all Internal STRs and will provide a reminder regarding tipping off requirements to the person making the report.

The Senior Compliance Officer / MLRO will investigate all reported suspicious transactions in light of all available information and document the findings, regardless of whether or not an external STR/SAR is made. All documented information will be retained with the Suspicious Transaction Reporting Form and retained in order to provide documentary evidence of the investigation process. Any further attempted activity on an account where an internal STR/SAR has been made must be reported to the Senior Compliance Officer / MLRO to ensure that appropriate action is taken in order to avoid tipping off.

External Reporting

An external STR/SAR is triggered when, after investigation by the Senior Compliance Officer / MLRO, a transaction, transaction pattern or account activity is deemed suspicious and suggests potential criminal activity. External STRs/SARs will be sent to the FIU.

8 Record-Keeping Procedures

The following records are to be kept for a period of at least five years:

- All necessary records on transactions, both domestic and international
- Records of the originator/payer information, and required beneficiary/payee information, on wire transfers, electronic fund transfers and other electronic payments; and,
- All records obtained through CDD including copies or records of official identification documents, account files and business correspondence, for at least five years after the business relationship is ended, or after the date of the occasional transaction.

The Company must provide the Regulator with a copy of all records, whenever the Company relocates the business or ceases business.

8.1 Guidance on Implementation

Records may be kept in any of the following forms:

- in physical files;
- in scanned form;
- in computerized or electronic form.

The Company should use a standardized approach to record keeping and must ensure that the approach used enables the quick retrieval of records.

8.2 Policy

The Senior Compliance Officer / MLRO is responsible for specifying which AML records must be retained and for ensuring that all such records are retained in accordance with Gammix STS

B.V.'s record-keeping policy.

Records may be held in paper-based and/or electronic form and may be stored by the Company. The Company will ensure that all AML records are retrievable without undue delay.

Records must be kept for a minimum of **5 years** (may be extended to 10 years if required by the Regulator).

8.3 Procedures & Documentation

Records are maintained for a period of at least 5 years. These records are the following: Outsourcing, Records of Client Due Diligence, Internal & external suspicious transaction reports, AML Training, AML Policy.

9. Awareness and Training

The Company must ensure that all staff receive adequate AML/CFT training in order that they might understand the risks and their own responsibilities as regards the prevention and mitigation of ML/TF risks. The training provided may include both general and role-specific training.

After the training each attendee must undergo an assessment to evaluate their recently acquired AML/CFT knowledge. If a score of at least 75% is not achieved, attendees will be required to re-sit the test and/or repeat the training.

Every year on the anniversary of their initial training and assessment all staff must attend refresher training. Any changes to relevant regulations, policies or procedures should be covered within the scope of this annual training.

9.1 Guidance on Implementation

All employees should be made aware of:

- Risks of money laundering and terrorist financing relevant to the business, the applicable legislation and staff obligations and responsibilities under the legislation;
- The Company's Risk Assessment methodology and mitigating policies, controls, and procedures.
- The identification of potentially suspicious transactions or activity; and,
- Red flags or indicators of money laundering or suspicious activity.

All the above-mentioned information should be made readily available to all employees to enable them to refer to such information as and when appropriate throughout the conduct of their duties.

Additionally, training should be of a more practical nature rather than simply theoretical. This means that the training provided should make references to real-life situations such as, for

instance, the steps to be followed when accepting Clients, the handling of high-risk Clients and the behavior to be adopted when faced with a request for a transaction which is suspicious.

The Company needs to determine the method in which training is to be delivered, as the most appropriate method may vary from one organization to the other. The method generally depends on the size of the organization. Online learning systems can often provide an adequate solution for general training to all employees who deal with clients, while focused classroom training for higher risk areas can be more effective.

It is vital to maintain comprehensive records of training sessions which, should include:

- a) the date on which the training was delivered;
- b) the nature of the training;
- c) the names of employees receiving the training;
- d) the results of any assessment undertaken by employees; and
- e) a copy of any handouts or slides.

9.2 Policy

Gammix STS B.V.'s Senior Compliance Officer / MLRO is responsible for ensuring that all relevant staff received training that effectively communicates Gammix STS B.V.'s AML and CFT responsibilities and the policies and procedures that are operated to ensure that those responsibilities are met.

Relevant persons

Relevant staff include the staff of the Company who handle or are managerially responsible for the handling of Client on-boarding and service provision.

Training

Training will be designed to ensure that all relevant staff are made aware of the risk of the Company being used for the purposes of financial crime, the consequences for the firm (as well as staff personally), the requirement to operate systems and controls to mitigate such risk and the requirement to report suspicious activity / transaction to the Senior Compliance Officer / MLRO.

The frequency of the provision of AML training will be determined using a risk-based approach, with those who may be at greatest risk from handling suspicious transactions, or who need to be kept up-to-date with changing vulnerabilities and trends, receiving training at more frequent intervals; relevant staff who are close to transaction processing activity are prioritized for training which may be more detailed in content than the training provided for other staff.

Where applicable, provision for AML training will be made in the contractual arrangements, or Service Level Agreements, between Gammix STS B.V. and its partners.

Senior Compliance Officer / MLRO Training

The MLRO will keep up to date with legislative changes and on international level and industry standards in order to guide and develop appropriate training for relevant staff.

9.3 Procedures & Documentation**Relevant persons**

The Senior Compliance Officer / MLRO will maintain a record of Gammix STS B.V.'s staff, and their positions within the company, for use when deciding which individuals are 'relevant staff' and, further, which will require more frequent and more detailed training due to the nature of their specific role.

Training

All relevant staff will be provided with an awareness of Gammix STS B.V.'s AML policies and processes through the provision of AML training. Relevant staff will be provided with initial AML training within one month of their taking up relevant activities on behalf of Gammix STS B.V.'s. Priority is given to those staff responsible for handling or managing the handling of transactions or Client accounts.

All relevant staff must acknowledge that they have read and understood the training that is provided, to be recorded in the AML Staff Training Log.

The frequency of training provided to each staff member is determined by the Senior Compliance Officer / MLRO with reference to the staff member's role. Refresher training is repeated at appropriate intervals. Relevant staff are assessed on the AML training received.

Training materials are updated by the Senior Compliance Officer / MLRO when required to reflect new developments. Training materials and records are retained in accordance with the Company's record-keeping policy.

AML training will be delivered to relevant staff and will include the following elements:

1. Legal and regulatory obligations under the relevant law;
2. Practical means of identifying unusual and suspicious transactions; and
3. Internal processes and advice on how to act when presented with suspicious activity.

Senior Compliance Officer / MLRO training

The Senior Compliance Officer / MLRO will receive external training as appropriate and is required to evidence, to the Board, their further professional development (using the MLRO Annual Report).

9.4 Anti-Bribery & Corruption Policy

The Company has embedded this Anti-Bribery & Corruption (ABC) Policy within the main AML Policy under this section. It outlines the commitment of Gammix STS B.V. to conducting its business activities in an ethical and lawful manner. The Company is dedicated to preventing bribery and corruption in all its operations and is committed to fostering a culture of integrity, transparency, and compliance.

The Company prohibits all forms of bribery and corruption, whether direct or indirect, and expects its employees, associates, contractors, and business partners to adhere to the highest standards of integrity and ethical behavior. This part of the policy applies to all employees, contractors, agents, suppliers, partners, and any individual or entity associated with the Company's operations, regardless of their role or position.

Definitions

Bribery: The offering, giving, receiving, or soliciting of any item of value (including but not limited to money, gifts, favors, entertainment, or services) to influence the actions of an individual in a position of trust or authority.

Corruption: The abuse of power or authority for personal gain, often involving bribery, embezzlement, fraud, or other unethical practices.

Associated Persons: Any individual or entity that has a business relationship with the Company, including employees, contractors, agents, suppliers, partners, and third-party intermediaries.

Prohibited Conduct

- a) **Bribery and Corruption:** No employee or associated person shall engage in any form of bribery, corruption, or unethical behavior. This includes offering, promising, giving, receiving, or soliciting bribes or other improper benefits.
- b) **Gifts and Hospitality:** Employees and associated persons must not offer or accept gifts, hospitality, or entertainment that could be seen as an attempt to influence business decisions or compromise the recipient's judgment.
- c) **Facilitation Payments:** Facilitation payments (small unofficial payments to expedite routine processes) are strictly prohibited. Employees and associated persons must not make or accept such payments.

The Company is committed to conducting thorough due diligence on all third parties before entering into business relationships with them. This includes assessing their integrity, reputation, and compliance with anti-bribery laws. Violations of this policy will not be tolerated and may result in disciplinary action, up to and including termination of employment or business relationships. In severe cases, legal action may be pursued. This policy will be reviewed periodically to ensure its effectiveness and relevance. Any necessary updates will be made to reflect changes in laws, regulations, and the Company's operations.

10. The Screening Process

The screening of potential Clients against sanctioned persons, against PEPs and against adverse media is conducted by Gammix STS B.V. via a 3rd party tool, a holistic and seamless Client Due Diligence software.

Sanctions and PEP screening result: on each possible match by selecting the entity result, positive hits. Adverse Media screening result: links are provided for the Company to analyze and investigate. All links besides the first ones, are highlighted, implying that these links have not as yet been accessed. By selecting any link, the Company will be directed to the actual article.

To screen Clients, the Company selects the screening icon and inserts the Client details requested. Once this is done, the Company will be presented with the possible results together with searches conducted via third party screening as well as targeted google searches. In addition to the identification and verification procedures, external search checks will be performed on the Client through the 3rd part tool's platform. Selecting the search engine item link shall direct the Company to another screen providing the actual information found within that link.

The Company is obliged to undertake measures at law aimed at combating terrorism, terrorism financing and the financing of the proliferation of weapons of mass destruction. This includes obligations emanating from the National Interest (Enabling Powers) Act relating to sanctions screening, freezing of assets, and reporting.

11. Sanctions Lists

11.1 Guidance on Implementation

The Company must ensure compliance with United Nations ("UN") Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing and in particular must freeze without delay the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either:

- (i) designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN, including in accordance with resolution 1267 (1999) and its successor resolutions; or,
- (ii) designated by that country pursuant to resolution 1373 (2001).

Further to this, the Company must ensure compliance with UN Security Council resolutions relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing and, in particular, must freeze without delay the funds or other

assets of, and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated by, or under the authority of, the UN Security Council under Chapter VII of the Charter of the UN.

The Company must ensure that adequate systems have been implemented in order to satisfy the requirements above, not only at the point of Client/Client onboarding, but on an on-going basis.

11.2 Policy

Sanctions list screening is the responsibility of the Senior Compliance Officer / MLRO. The performance of the screening procedures may be delegated or outsourced.

In obtaining, applying, and disseminating government and FATF findings, the Senior Compliance Officer / MLRO ensures that all Clients and business partners (e.g. 3rd parties) with whom a business relationship is established, are subject to due diligence procedures that ensure screening against relevant sanctions lists, such as:

- OFAC (Office of Foreign Assets Control);
- EU (European Union);
- OFSI (Office of Financial Sanctions Implementation);
- UN (United Nations); and
- Australian Governments Dept. of Foreign Affairs (DFAT).

Sanctions screening will form part of the initial due diligence procedures as well as the ongoing monitoring of Clients and business partners as detailed in Annexes III and IV below. 'False positives' are investigated, and any true sanction matches reported to the Senior Compliance Officer / MLRO immediately. Staff are required to report where they have knowledge of or a suspicion that financial sanctions measures have been or are being contravened. Senior Compliance Officer / MLRO can be contacted through the following email address:

compliance@kmlpartners.com

11.3 Procedures and Documentation

All Clients shall be subject to Sanctions screening once this is actively implemented as part of the initial due diligence procedures, with all Clients being rechecked regularly as part of the ongoing monitoring of Clients.

Staff responsible for performing sanctions checks will receive specific training. Matches will be investigated by staff in order to identify true matches from those that are 'false positive'. All true sanctions matches must be reported to the Senior Compliance Officer / MLRO immediately, using the Internal Suspicious Transaction Reporting Form and followed up by an email thereafter.

12. Politically Exposed Persons

In addition to performing normal CDD measures, the Company must have appropriate risk-management systems to determine whether the Client or the beneficial owner is a Politically Exposed Person, ("PEP") or an immediate family member or close associate of the PEP.

12.1 Guidance on Implementation

As stated above, it is the responsibility of the Company to ensure that appropriate risk measures have been implemented to identify and manage the risk of any PEP relationship. Where a PEP connection has been identified, the Company must make reasonable efforts to ascertain the PEP's Source of Wealth ("SOW") and Source of Funds ("SOF") / income is not from illegal activities and where appropriate review the Client's credit and character and the type of transactions the Client would typically conduct. The Company must not accept or maintain a business relationship if the Company knows or must assume that the funds are derived from corruption or misuse of public assets.

Where a PEP connection is identified, the Company must ensure it has obtained approval from the Senior Compliance Officer / MLRO. Where a Client has been accepted and the Client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, the Company must further obtain senior management's approval to continue the business relationship.

Where the Company is in a business relationship with a PEP, it must conduct enhanced ongoing monitoring of that relationship.

12.2 Policy

When conducting risk assessments for new Clients, products, or features, Gammix STS B.V. must evaluate several factors to identify potential risks associated with their use. One significant consideration is the possibility of these products being exploited for money laundering by PEPs.

New Clients:

- **Background Checks:** Conduct thorough due diligence on new Clients, particularly to determine if they are PEPs or have any associations with PEPs.
- **Enhanced Due Diligence (EDD):** Implement enhanced scrutiny and monitoring for Clients identified as PEPs due to their increased risk of involvement in money laundering.
- **Risk Profiling:** Develop risk profiles for new Clients, considering factors such as their source of wealth, geographical location, and business activities, especially focusing on those who are or may be PEPs.

New Products:

- **Product Vulnerability Assessment:** Evaluate the inherent risks associated with new products, particularly how they might be misused for illicit activities, including money laundering by PEPs.
- **Control Measures:** Design and implement control measures to mitigate identified risks, such as transaction limits, monitoring mechanisms, and reporting requirements.
- **Regulatory Compliance:** Ensure that new products comply with anti-money laundering (AML) regulations and guidelines, including those specifically addressing the risks posed by PEPs.

New Features:

- **Feature Analysis:** Analyze new features for potential vulnerabilities that could be exploited by money launderers, particularly PEPs.
- **Usage Monitoring:** Develop systems to monitor the usage of new features to detect unusual or suspicious activities indicative of money laundering.
- **User Education:** Inform and educate users about the proper use of new features and the importance of complying with AML regulations, especially regarding transactions involving PEPs.

12.3 Procedures and Documentation

All applicants for business shall be required to confirm whether they qualify as PEPs. The declaration shall be recorded upon registration. In addition, a third-party check shall be carried out on each person to assess whether the person in question is a PEP.

Annex I – Senior Compliance Officer / MLRO Job Description

Senior Compliance Officer / MLRO

Responsibilities

Gammix STS B.V. is responsible for appointing a Senior Compliance Officer / MLRO of appropriate seniority with access to the resources required to effectively perform the role. Resources include time, support staff, the freedom and independence to act on authority, and access to relevant data / information.

In summary, the Board of the Company delegates the following high-level responsibilities to the Senior Compliance Officer / MLRO:

- Establishing and operating appropriate risk-based internal policies, procedures, and controls to prevent money laundering or terrorist financing, consistent with legal and regulatory requirements as set out in international provisions.
- Reviewing, updating, and approving AML and CFT policies based on an assessment of risk and its management, ensuring that such assessments are kept up to date.
- Ensuring that priority is given to the implementation of AML and CFT policies and take ultimate responsibility for the development and operation of procedures that implement policy.
- Maintain up-to-date documentation detailing the risk-based AML and CFT arrangements operated by the Company.

Senior Compliance Officer / MLRO Role

The Senior Compliance Officer / MLRO may delegate certain functions, in particular those related to the day-to-day monitoring of procedures and systems to detect suspicious activity, to suitable individuals in Gammix STS B.V. (where resources are available).

It is the Senior Compliance Officer / MLRO's ultimate managerial responsibility to ensure that the provisions of this Policy are enforced. Where the MLRO delegates any activities, they will remain accountable for the operation of the delegated functions. The Senior Compliance Officer / MLRO may hold other senior management responsibilities within entities of Gammix STS B.V., to the extent that they do not interfere with their ability to conduct the Senior Compliance Officer / MLRO duties.

In the absence of the Senior Compliance Officer / MLRO for a period of less than 12 weeks, the Senior Compliance Officer / MLRO duties will be temporarily performed by a suitably experienced and qualified individual from within Gammix STS B.V. The MLRO will always remain reachable and in close contact with the head office. Should the position of the Senior Compliance Officer / MLRO become vacant (i.e. the MLRO be absent for a period of 12 weeks or more in a consecutive 12-month period), the Board will appoint another suitably qualified individual as its MLRO / Senior Compliance Officer.

POSITION RESPONSIBILITIES

Establishing and supervising AML and CTF systems and controls

Developing and overseeing the implementation of appropriate **AML and CTF policies and procedures**.
 Determining the level of **resources** required to execute appropriate AML and CTF policies and procedures.
 Maintaining and developing the **risk-based approach** to AML and CTF arrangements - carrying out regular **assessments** of the adequacy of systems and controls.
 Reviewing the output from the **suspicious activity monitoring** processes.
 Ensuring that AML and CTF requirements are considered as **part of the development** of new products, or service changes.
 Obtaining Board approval for significant **process changes**.
 Ensure that policies and procedures are accurately documented in the **AML Policy** which should be available to staff and used to guide training.
 Ensure that the Board are kept informed of the **money laundering risks** posed by the business and its activities, and how these are managed and mitigated.
 Reporting to the Board on a regular basis detailing the operation and effectiveness of the systems and controls used to combat financial crime.
 Documenting and ensuring that any actions recommended by the Board are implemented. Arranging and assisting with regulatory visits and audit inspections.

Maintaining relevance of the AML systems

Regularly reviewing developments in applicable **legislation and guidance** (domestic and international where the business is involved).
 Ensuring that **policies are updated** to meet changing regulatory and business requirements.
 Ensuring that the operation of systems and controls are **monitored** and that they implement policy. Ensuring that relevant staff are provided with **training** appropriate for their position (frequency and content) and that all new staff receive training within the specified period. Ensure that **training materials** remain up-to-date and relevant to the business.

Reporting suspicious activity

Investigating **internal Suspicious Activity / Transaction Reports (SARs/STRs)**.
 Deciding, following investigation, whether the internal report gives rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion and submitting an **external STR/SAR to the FIU** where appropriate.
Documenting the reasons for not submitting an external STR to FIU and/ where an internal report has been made, considered and deemed not to be suspicious.
 Maintain a **filing system** of all internal STRs, separating between those reported to FIU and those not.
 Ensure that relevant **records are retained** for the prescribed periods. Where required be the main **point of contact** for law enforcement officials.

Annex II – Risk Mitigation Matrix and Risk Factors

Risk Assessment and Mitigation Matrix

The Company has a Partner Risk Assessment form, which is a separate excel file in order to risk assess each Client.

Risk Factors Table

The following represent risk factors relevant to Gammix STS B.V.'s current service offerings that could indicate Money Laundering or Funding of Terrorism as per the risks highlighted in the table above. Other risk factors can be found under section 3.2 and 4.2 of this AML Policy.

Risk Factor	Risk Factor	Risk score	Mitigating Reasons
Client	PEP/Sanctioned	10	None
Client	Clients based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime, or drug production/distribution	10	None
Geographical Area	Merchant's Clients are based in or conducting business in, or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime, or drug production/distribution	10	None

Process for Determining Client Risk

The activities of each Client are assessed in relation to the risk factors above and the said assessment is recorded in the Partner Risk Assessment Form. A proposed risk assessment of Very Low, Low, Medium, High or Very High is recorded.

Members of staff may take into account any applicable mitigation reasons set out in the table above, in which case the reasons for the mitigation are recorded in the said Partner Risk Assessment Form. The risk assessment may be revised on the basis of these mitigations subject to the consideration that a risk may never be assessed as low where:

- i. the client is non-face-to-face (save for those instances detailed in the section entitled "Simplified Due Diligence" a) or b))
- ii. the client is a PEP
- iii. the client is from or is active in a high-risk jurisdiction

Annex III – Client Due Diligence

The Company has established systematic procedures for identifying an applicant for business and ensuring that such identity of its Directors / UBOs are verified on the basis of documents, data or information obtained from a reliable and independent source.

Persons subject to Identification and Verification

For the purposes of the services provided the following legal and/or natural persons shall be subject to identification and verification procedures as stipulated below.

- i. The Client being the natural person who is registered with the Company to which services are provided by the Company;
- ii. A company or legal entity which is considered to be an intermediary of the Company to which services are provided by the Company;
- iii. The Ultimate Beneficial Owners of a Company or legal entity which is considered to be an intermediary of the Company;
- iv. The Directors of a Company or legal entity which is considered to be an intermediary of the Company;

For the purposes of the above that the **Ultimate Beneficial Owner** (UBO) of a body corporate or a body of persons includes all natural persons who ultimately own or control, whether through direct or indirect ownership or control, 25% or more of the shares or voting rights in the Company or legal entity in relation to which services are or will be provided.

Provided that natural persons who ultimately own or control a company that is listed on a regulated market which is subject to disclosure requirements consistent with Community legislation, or equivalent international standards shall be excluded from verification requirements. In such a case Option B should be selected in Annex B on the Client On-boarding Form.

Provided further that in the case of a trust where beneficiaries have not been determined, due diligence will be carried out on any class of persons in whose main interest the trust is set up.

For the purposes of the above that the “**beneficial owner**” of a body corporate or a body of persons includes all legal persons who own or control, whether through direct or indirect ownership or control, 25% or more of the shares or voting rights in the Company or legal entity in relation to which services are or will be provided,

Provided that companies that are listed on a regulated market or otherwise subject to financial business regulation which are subject to disclosure requirements consistent with Community legislation, or equivalent international standards shall be excluded from verification requirements. In such a case Simplified Due Diligence should be followed for Client On-boarding.

Provided that for Directors, the Company shall only be required to identify such persons and

hence, notwithstanding anything to the contrary, no verification shall be required to be collected.

In order to be able to identify each of the persons subject to identification and verification as part of the on-boarding process, the applicant for business is to provide an up-to-date organogram to the Company which is to be signed by an authorized official of the applicant, both at on-boarding and each time that there is a significant change in ownership.

Due Diligence for Natural Persons

Where the persons subject to identification and verification are natural persons, the following information shall be obtained in all cases in relation to identification and verification:

OPTION A:

1. Verification of Details - one of the following:
 - 1.1. a valid unexpired passport; or
 - 1.2. a valid unexpired national or other government-issued identity card; or
 - 1.3. a valid unexpired driving license.
2. Verification of Residential Address - one of the following not older than six (6) months:
 - 2.1. a recent statement from a recognized credit institution;
 - 2.2. a recent utility bill;
 - 2.3. correspondence from a central or local government authority, department, or agency;
 - 2.4. any government-issued document where a clear indication of residential address is provided; or
 - 2.5. any other document as may be specified in sectoral implementing procedures issued by the FIU.

In addition to the above, one of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Client's risk has been assessed as '**Medium Risk**' and two of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Client's risk has been assessed as '**High Risk**' or '**Very High Risk**' as follows:

OPTION 1: One of the following

1. a professional reference (warranted lawyer or auditor)
2. a bank reference
3. an additional recent statement from a recognized credit institution;
4. an additional recent utility bill;
5. correspondence from a central or local government authority, department, or agency;
6. any government-issued document where a clear indication of residential address is provided; or
7. any other document as may be specified in sectoral implementing procedures issued by the FIU.

OPTION 2:

1. *The first payment be made from a bank set up in the EU or of a reputable jurisdiction with similar standards of banking regulation. For the purposes of this option 'bank' may also include financial institution, payment institution or electronic money institution.*

OPTION 3:

1. *Determination of source of wealth and source of funds signed by a recognized accountant/auditor.*

OPTION 4:

1. *Police conduct certificate*

OPTION 5:

Require that the documentation provided in OPTION A.2 and A.3 above is certified by a legal professional, accountancy professional, notary, person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction. Such certification should be evidenced by a written statement stating that:

- the document is a true copy of the original document;
- the document has been seen and verified by the certifier; and
- the photo is a true likeness of the applicant for business or the beneficial owner, as the case may be.

The certifier must sign and date the copy document (indicating his name clearly) and clearly indicate his profession, designation, or capacity on it and provide his contact details.

Provided that in all cases where the applicant, beneficiary owner or the ultimate beneficial owner is a PEP, Gammix STS B.V. will proceed to end the relative business relationship.

Due Diligence for Legal Persons

Part A

Where the persons subject to identification and verification are legal persons, the following information shall be obtained in all cases in relation to identification and verification:

- a) to identify the following:
 - i) the legal person's official full name;
 - ii) the legal person's registration number (if applicable);
 - iii) the legal person's date of incorporation or registration; and
 - iv) the legal person's registered address or principal place of business.
- b) To verify the information and legal status mentioned under Part A(a), the most recently dated version of any of the following documents must be obtained:

- i) Memorandum and Articles of Association; or
- ii) Certificate of Incorporation; or
- iii) Signed declaration by an authorized official of the applicant for business; or
- iv) Company registry search, which includes confirmation that the private company has not been, and is not in the process of being dissolved, struck off, wound up or terminated; or
- v) Latest annual return; or
- vi) Other statutory document.

In relation to the above, the staff member must view the original document, a certified copy of the original or a downloaded copy from the official registry website. Certification should be carried out by the company secretary, a director or an officer occupying an equivalent position or by the Registrar of Companies or a person occupying an equivalent position in a foreign jurisdiction.

Alternatively, certification may be carried out by a legal professional, accountancy professional, notary, person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction.

The certifier must sign and date the copy document (indicating his name clearly) and clearly indicate his profession, designation, or capacity on it and provide his contact details.

The certified copy of the original or the copy downloaded from the official registry website shall be retained by Gammix STS B.V. Where an original document is viewed, Gammix STS B.V. shall keep a true copy of the document, signed, and dated by an officer of the subject person, on file.

Alternatively, identification and verification may be carried out by obtaining one or more additional (different) documents from amongst the list provided in Part A (b) above which verify the information obtained through the first set of documentation provided.

In addition to the above, one of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Client's risk has been assessed as '**Medium Risk**' and two of the following Options shall be satisfied for the purposes of Enhanced Due Diligence where the Client's risk has been assessed as '**High Risk**' as follows:

OPTION I:

1. The latest audited financial statements; provided that in the case of Enhanced Due Diligence, this shall only be required if allowed by the jurisdiction of the applicant for business.

OPTION II:

1. The first payment be made from a bank set up in the EU or in any other jurisdiction with similar standards of banking regulation. For the purposes of this option 'bank' may also include financial institution, payment institution or electronic money institution.

OPTION III:

1. Certificate of good standing or a certificate of incumbency, not older than six (6) months.

OPTION IV:

1. A professional reference signed and duly dated by a legal professional, accountancy professional or notary.

Part B

Post identification and verification of the Legal Person, the Company shall also identify all the directors. This shall be done by either of the following:

- i) referring to the list of directors contained in the most recent version of the Memorandum and Articles of Association; or
- ii) by performing a company registry search provided that the officers of the company are listed therein; or
- iii) by obtaining a copy of the directors' register of the company.

Part C

Upon the identification of the shareholders and Ultimate Beneficiary Owners' details as a result of the Organogram and documentation provided as mentioned above, the staff member shall perform and record the Due Diligence provided for natural persons in respect of such Ultimate Beneficiary Owners with particular regard to non-face-to-face procedures if required:

Provided that should the applicant's operations be regarded as high risk, shareholders having between 10% but less than 25% of the control in the applicant, may be required to provide for identification details including but not limited to First Name, Last Name and Date of Birth.

In instances where the documentation provided under Part A(b) does not identify the shareholders and the Ultimate Beneficiary Owners, the applicant for business has to supply any of the following documents:

- i) Latest share register; or
- ii) Signed declaration by an authorized representative of the applicant for business, which declaration should include sufficient details to enable the subject person to identify the shareholders and the Ultimate Beneficiary Owners.

For avoidance of doubt, no proof of address will be requested of shareholders holding an interest between 10%, but less than 25%.

Languages

All documents are to be provided in English (or any other language which any official of the Company understands). Certified translations are to be translated of documents in other languages.

Client Terms and Conditions

The Client Terms and Conditions includes a declaration by an authorized representative of the applicant for business as to whether they have:

- a) ever been convicted of an offence (other than a minor traffic offence);
- b) ever been adjudged bankrupt;
- c) ever been the subject of an investigation by a government, professional or other regulatory body;
- d) ever been a director, shareholder, officer or manager of a business entity which has been the subject of an investigation as aforesaid
- e) ever been a director, shareholder, officer, or manager of a business entity which has been adjudged bankrupt compulsorily wound up or has made any compromise or arrangement where its creditors or has otherwise ceased trading in circumstances where its creditors did not receive or have not yet received full settlement of their claims; and
- f) unless otherwise disclosed in the terms and conditions, ever had, or currently has any direct or indirect beneficial interest in or whether he ever was or currently is a director of any other company.

Client Risk Assessment

Each Client is subject to a risk assessment and subsequently rated as Very Low Risk, Low Risk, Medium Risk, High Risk or Very High Risk as set out in Annex II above.

For the purposes of such assessments additional information may be required from the Client.

Face-To-Face Transactions or Clients

In all instances of face-to-face onboarding, provided that the applicant does not provide certified true hardcopies or the originals of the documentations required as per the abovementioned procedures, the Company representative is to view the original document, make a hard copy of such document (printed scan/photograph etc.) and certify that this is a true copy of the original seen by him, while duly signing the document including the relevant date.

All instances of face-to-face clients will require any one of the following:

- a) Include an email on file confirming that a face-to-face meeting with the applicant for business duly occurred prior to onboarding;
- b) A certified true copy in original by an Gammix STS B.V.'s representative of an identification document of the applicant for business' representative, provided that such document was copied by a Company's representative himself; or
- c) Minutes of the meeting with the applicant for business' representative, signed and duly dated by the Company representative.

Timing of Due Diligence

Each client shall provide a copy of all documentation in order to assess that all the documentation is in order and to proceed with the onboarding.

In some instances, a corporate client (intermediary) may select to sign the Services Agreement prior to the carrying out of on-boarding to provide a commitment to eventual onboarding. In this case, no services are permitted, and no services shall be provided to the client and no transactions entered into prior to the carrying out of all due diligence procedures and prior to on-boarding.

In the event that due diligence documentation is not provided by the Client or it otherwise becomes obvious that the Client is not able to satisfy due diligence requirements, the Service Agreement or Client onboarding shall be stopped. The MLRO will consider the appropriateness of filing an SAR/STR.

Annex IV – Client Acceptance Policy

The Company or intermediary of the Company policy for acceptance of Clients takes into consideration the Risk Assessment and mitigation measures as well as the risk factors indicated in Annex II above.

Client Acceptance

The Company or an intermediary of the Company shall not accept the following clients:

- i. Clients that fail the relevant due diligence identification and verification controls set out in Annex III above;
- ii. Clients who themselves or their ultimate beneficial owners are excluded Clients listed below;
- iii. Clients who have in the past been reasonably associated or involved in criminal activities or other illegal activities may result from searches on the clients, beneficial owners and on any other person in relation to whom due diligence is carried out.

Excluded Activities

The Company or its intermediaries shall not accept the following types of business activities for any provision of services:

- i. Trading in Arms
- ii. Supplying Technology or Parts Connected with Defense
- iii. Providing Military Security Services
- iv. Clients resident in jurisdictions where the Company - or its affiliated Group Companies with whom service agreements are in place - are not authorized to provide gaming services.

Excluded Individuals

The Company or its intermediaries shall not accept the following persons:

- i. Sanctioned Individuals and/or entities;
- ii. Entities with bearer shares;
- iii. Entities where UBOs cannot be identified;
- iv. Persons who seek to set up a business relationship or conduct an occasional transaction in the name of third parties under an anonymous name or nickname;
- v. Clients having underlying Clients.

Risk-Based Approach for Accepting Clients

On the basis of the risk approach highlighted in Section 3 of the AML Policy and Annex II above, risk factors are taken into account to determine the risk of each Client (low, medium, or high). Different levels of Enhanced Due Diligence are applied in the event of Medium, High or Very High-risk assessments.

The manner in which the assessment is carried out is highlighted in Annex II above.

Annex V – Internal STR/SAR Form

Internal STR/SAR Form Template

The STR/SAR should be a prompt report and escalated to the FIU as soon as possible.

(Please send the Internal STR/SAR to the Senior Compliance Officer / MLRO and cc the Deputy MLRO if exist)

Reporter's details (this section is to be completed by the Reporter)	
Reporter's name:	
Reporter's email:	
Date:	
Department:	

Subject(s) of the STR/SAR (this section is to be completed by the Reporter)	
Client's business name:	
Relationship start & end date:	
Client's business address:	
Client's phone number(s):	
Client's email address:	
What is the reason for reporting?	
Non-Compliance with Requests?	
Other (please specify)	
What evidence is supporting your suspicion? <i>(Please add sources & links such as: transaction records, email correspondence, screenshots, etc.).</i>	

AML details (this section is to be completed by the Reporter)	
ID Number of the Director(s) / UBO(s):	
ID Expiry Date of the Director(s) / UBO(s):	
CDD / EDD Status:	
Status of business relationship:	
Services utilized:	
Reference nr. if linked to a previous STR/SAR:	

Activity Information (this section is to be completed by the Reporter)

Provide a comprehensive description of the suspicious activity, including dates, times, and any relevant transactions or behaviors observed. *It may be easier to export this as an excel document and attach.*

Supporting documentation attached (this section is to be completed by the Reporter)
When you escalate the internal SAR please attach in the email: ID, Proof of address documents, email correspondence, screenshots, etc.

Client Due Diligence Documents (ID / PoA):	Client Notes:
Client Communications Logs:	

Timeline of the Suspicious Activity / Transaction (this section is to be completed by the MLRO)

(The timeline should be detailed and sufficiently clear that someone not familiar with the activity or Company would understand it. Please avoid jargons and acronyms)

xx/xx/xxxx – Client started the onboarding process

xx/xx/xxxx – We verified ID, Proof of address of Director, etc.

xx/xx/xxxx – We found a negative adverse media regarding our Client (*include link if available, date and a short summary about the article*)

xx/xx/xxxx – Partner onboarding was stopped.

xx/xx/xxxx – An internal SAR was considered.

The information or other matter which gives the grounds for your knowledge, suspicion, or belief:

- Negative adverse media have found;
- No cooperation with our Due Diligence Documentation / Source of Wealth request.

MLRO Determination (this section is to be completed by the MLRO)

1. Did we find positive info online on the Client that would discharge our concerns?
2. Did we find any negative info found online or in the account history, data, behavior, documents etc., that would mean we clearly need to report?

I suggest we file this as an STR/SAR, but that will depend on the answers above.

A record of this STR/SAR together with all related documents will be kept by the Senior Compliance Officer / MLRO for at least five (5) years.

Annex VI – Abbreviations

AML	Anti-Money Laundering
AML Regulation	Regulations Concerning Anti-Money Laundering and Countering Terrorism Financing
CMP	Compliance Monitoring Program
CFT	Combating Funding of Terrorism
EU	European Union
KYC	Know Your Client
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
TF	Terrorist Financing
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
RBA	Risk Based Approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report

Annex VII – Signatory page

Gammix STS B.V.

Curacao, 19th May 2025

Signed by:



8737E2B30CE043E...

Analissa Mercedes Eustatius Heiland

Xecutive Corporate Management B.V. – Managing Director

Signed by:



E9C1A4A3F74E4ED...

Lorenza Godett

Xecutive Corporate Management B.V. – Managing Director

Signed by:



C844330A35E54B6...

Mark Cauchi

Key Compliance Officer