

Global Software Solutions N.V.

AML/CFT MANUAL

V. 1.0 - May 2025

Table of Contents

Revision History	2
Definitions and Abbreviations	3
1. AML/CFT Policy	6
1.1 Policy	6
1.2 Objectives	7
1.3 Scope	7
2. Regulatory Framework	8
2.1 National regulations	8
2.2 International regulation	9
3. Procedures	10
4. Risk Management	10
4.1 Risk assessment	10
4.2 Business risk assessment	11
4.3 Risk Classification	12
5. KYC Procedure	13
5.1 Due Diligence	13
5.2 Enhanced Due Diligence	14
5.3 Politically Exposed Persons	15
6. The Monitoring of Counterparty activities	15
6.1 Unusual activities	16
7. Reporting of unusual transactions	17
8. Compliance officer (CO)	17
9. Recordkeeping	17
10. Periodical review of AML/CFT policies	18
Contact Information	18

Revision History

Version #	Effective Date	Approving Official	Responsible Office	Next Review Date	Comments
1.0	May 28, 2025	eMoore N.V.	Compliance function	May 28, 2026	-

Definitions and Abbreviations

Anti-Money Laundering (“AML”)	All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Caribbean Financial Action Task Force (“CFATF”)	An organization of states and territories of the Caribbean territory that have agreed to implement common countermeasures against money laundering and terrorism financing. (www.cfatf-gaific.org)
Combating terrorist financing (“CFT”)	Combating the Financing of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
Counter proliferation Financing (“CPF”)	Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.
Counterparty	Any business counterparty of the company with whom an agreement has been signed.
The Company	Global Software Solutions N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 121022.
Employee	Any person working for the Company.
Financial Action Task Force (“FATF”)	An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist

	financing and other related threats to the integrity of the international financial system. (www.fatf-gafi.org)
Financial Intelligence United ("FIU")	Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of unusual transaction reports (UTR) and other information regarding potential money laundering or terrorist financing.
Know Your Client ("KYC")	The mandatory process of establishing the identity of a counterparty and the verification thereof.
Money Laundering ("ML")	A process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.
Politically Exposed Persons ("PEP")	A person entrusted with a prominent public function, such as a senior political figure. Individuals closely related to this person, for instance immediate family members and close associates, are also considered PEPs. PEPs are classified as a Money Laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.
Prohibited Countries	Jurisdictions prohibited under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, jurisdictions restricted by decision of the Company's managing director at a certain moment when and where still applicable, as well as countries mentioned on the FATF blacklist or on which any financial sanctions has been imposed by the EU/ U.N. and/or the OFAC.
Proliferation Financing ("PF")	The act of providing funds or financial services which are used, in whole or in part, for the manufacture,

	acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
Service	Services provided by the B2B operator as outlined in the agreement with the Counterparty.
Terrorism Financing ("TF")	The process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities.
Unusual transaction	Any financial or operational activity conducted by a counterparty that is inconsistent with their known behavior, business profile, or legitimate operations, and may indicate potential fraud, money laundering, or regulatory evasion.

1. AML/CFT Policy

1.1 Policy

ML, TF and PF are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Entities involved in ML, TF and PF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such entities must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

TF may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures.

PF may involve the financing for the sale, transfer, export, of weapons of mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a significant threat to international peace and security, as identified by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the CFT measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable

national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

1.2 Objectives

This Policy outlines the AML/CFT/ CPF strategy of the Company in order to:

1. ensure that statutory and regulatory obligations to prevent ML, TF and/or PF are met, taking positive action to minimize risk of the Company's products and services being used for the purpose of laundering funds and using proceeds of criminal activity, or terrorist financing;
2. ensure that the Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with ML, TF and/or PF;
3. terminate any relationships where the Counterparty conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations; and
4. comply with the Company's AML/CFT/CPF obligations based on national and international regulations.

1.3 Scope

This Policy applies to all persons working for the Company or on the Company's behalf in any capacity, including Employees, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external contractors, third-party representatives and business partners, sponsors, or any other person associated with the Company that falls within the scope of the Company's AML Policies.

This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations. Failure of an Employee to comply with the procedures defined within this Policy may lead to disciplinary action.

2. Regulatory Framework

2.1 National regulations

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

1. The National Ordinance on Money Laundering (P.B. 1993, no. 52);
2. The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2024 no.41(N.G.2017, no. 92) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
3. The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G.2024 no.41 (N.G. 2017, no. 99) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
4. The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
5. Kingdom sanction act (N.G. 2016, no. 54)

6. Sanctions National Ordinance (N.G. 2014, no. 55) together with all related amendments thereto and all related National decrees containing general measures and Ministerial Decrees with general operations;
7. National Ordinance on the Obligation to report Cross-border Money Transportation N.G. (2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

2.2 International regulation

As a member of the FATF and of the CFATF Curaçao is meeting international standards by regularly implementing these standards in its national legislation. On an international level, the FATF plays an important role in the combating of ML and the TF and proliferation of weapons of mass destruction.

The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

3. Procedures

To be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself when providing Services to its Counterparties. These procedures cover the following standards:

- Risk management
- Know Your Customer Procedure
- Reporting of Unusual Transactions
- Recordkeeping

4. Risk Management

4.1 Risk assessment

The possibility of online gaming being used by criminals to assist ML, TF and/or PF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

The Company takes the following steps to manage its risks appropriately:

- i. identifying the ML, TF and PF risks relevant to the Company;
- ii. assessing the level of risk.
- iii. understanding the impact of the risk;
- iv. designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- v. monitoring and improving the effective operation of these controls and identifying any weaknesses; and
- vi. recording what has been done and why.

In view of the above, the Company has conducted a risk assessment to identify and analyze the AML risks faced by the Company and to ensure that the identified risks are properly mitigated and resources adequately invested.

4.2 Business risk assessment

The following table provides an overview of the AML risks identified when rendering services:

Risk ID	Risk Description	Likelihood	Impact
AMLBB001	Failure to verify ultimate beneficial ownership (UBO) of client operators	4	5
AMLBB002	Inadequate onboarding checks for B2C operator clients	4	4
AMLBB003	Delayed or inaccurate suspicious activity reporting (SAR)	3	5
AMLBB004	Inadequate monitoring of client transaction patterns	4	4
AMLBB005	Failure to screen clients against PEP and sanctions lists	3	5
AMLBB006	Poor documentation and record-keeping of AML processes	3	4
AMLBB007	Staff unaware of AML red flags due to inadequate training	4	4
AMLBB008	Clients operating in or serving high-risk jurisdictions	4	5
AMLBB009	Lack of periodic risk assessment updates	3	4
AMLBB010	Inconsistent application of enhanced due diligence (EDD)	4	5
AMLBB011	Failure to identify nested or layered corporate structures	3	4
AMLBB012	Technology gaps in detecting AML patterns or anomalies	3	4
AMLBB013	Manual AML reviews causing backlog and exposure	4	4
AMLBB014	No central system for tracking AML case management	4	4
AMLBB015	Failure to update AML policy in response to regulatory change	3	5

Mitigation strategy and residual risk towards AML risk

The following tables show the Mitigation strategy to be implemented and the effectivity rate, followed with the activities to reduce residual risk, the risk score, the residual risk score and the residual risk level.

Risk ID	Mitigation Strategy	Mitigation control effectiveness
AMLBB001	UBO verification tools, document validation checks	6
AMLBB002	KYC automation, onboarding checklist enforcement	6
AMLBB003	Automated SAR generation, MLRO escalation triggers	7
AMLBB004	Deploy real-time monitoring, anomaly detection	6
AMLBB005	Integrate global watchlist screening system	6

AMLBB006	Centralized document repository, audit trails	6
AMLBB007	Mandatory AML training, annual refresher sessions	5
AMLBB008	Jurisdiction screening and geo-fencing alerts	6
AMLBB009	Annual risk assessment with change indicators	5
AMLBB010	EDD workflow automation and exception monitoring	6
AMLBB011	Legal structure validation tools, hierarchy mapping	6
AMLBB012	AML analytics system, pattern recognition models	5
AMLBB013	AML case load dashboard, triage prioritization	5
AMLBB014	Case management platform with status tracking	6
AMLBB015	Subscription to legal updates, internal SOP refresh	5

Risk ID	Activities to reduce Residual risk	Risk score	Residual risk score	Residual risk level
AMLBB001	Enhanced onboarding for corporate entities, automated UBO check tools	20	14	Medium
AMLBB002	Revise checklist, enforce KYC preconditions	16	10	Medium
AMLBB003	Expand alert criteria and update SAR triggers	15	8	Medium
AMLBB004	Link client activity to benchmarked patterns	16	10	Medium
AMLBB005	Daily sanctions screening updates, audit logs	15	9	Medium
AMLBB006	Quarterly record reviews and audit sampling	12	6	Low
AMLBB007	Introduce AML e-learning tracking system	16	11	Medium
AMLBB008	Monitor country risk shifts and client exposure	20	14	Medium
AMLBB009	Integrate auto-risk rating engine	12	7	Medium
AMLBB010	Deploy EDD case monitoring reports	20	14	Medium
AMLBB011	Include corporate mapping in onboarding forms	12	6	Low
AMLBB012	Deploy unsupervised learning models	12	7	Medium
AMLBB013	Expand analyst team and triage support	16	11	Medium
AMLBB014	Centralize workflows with escalation paths	16	10	Medium
AMLBB015	Quarterly review of regulatory horizon and SOPs	15	10	Medium

4.3 Risk Classification

Upon registration, the Company makes a risk classification for each Counterparty. The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

The level of due diligence that should be performed on the Counterparty is determined based on the risk classification above.

Type of Customer	Monitoring frequency
Counterparties who are under active investigation or suspected in ML/TF or other fraudulent activity arising after onboarding	Daily
PEPs, which are deemed to present a high risk	Daily
High-Risk Counterparties, PEPs with lower relative risk and active Counterparties from high-risk jurisdictions	Weekly (or upon a material change)
Medium Risk Counterparties	Every six months (or upon a material change)
Low Risk Counterparties	Annually (or upon a material change)

5. KYC Procedure

5.1 Due Diligence

The Company verifies the identity of its Counterparties before or during the course of establishing a business relationship. The Company has a formal procedure in place to conduct KYC/Due Diligence checks. In most cases the Counterparty is a legal entity or legal arrangement. For identification and verification purposes of such Counterparties, the Company may request the following documents for agreements with a contract value threshold of USD \$50,000.00 or more::

1. a recently issued excerpt from the trade registry or a similar document evidencing the existence and Good Standing of the Counterparty;
2. a list of authorized signatories (in case controllers are not stated in the latter document).

For the purpose of the identification of corporate directors acting on behalf of the Counterparty, the Company may request the following documentations:

1. a recently issued excerpt from the trade registry or a similar document evidencing the existence and Good Standing of the Counterparty;
2. a list of authorized signatories (in case controllers are not stated in the latter document)

Regardless of the contract value, *all* Counterparties — including those with agreements below USD \$50,000.00 — are subject to screening using automated screening tools and open-source methods such as Google searches.

Based on the outcome of the due diligence review, it is determined whether additional documentation is required and whether the business relationship can be established.

5.2 Enhanced Due Diligence

In certain instances the Company might require further in depth investigation of the prospect Counterparty. For example:

- when the prospect Counterparty is regarded as a high risk due to it being established in a country designated as a high-risk country by the FATF,
- when the provided identification information is considered unsatisfactory or is suspected to be fraudulent;
- or in case of further adverse findings following the first screening.

The Company will conduct a further enhanced investigation on the identity of the prospect Counterparty and the specific findings. This process entails but is not limited to the following actions:

- request for further corporate documentation establishing the purpose of the entity;
- verifying the disclosed details against certain (public or private) databases (e.g. Interpol, international blocked lists);
- request additional documentation (e.g. Certificates of Registration or status of licenses or audited financial reports);

Failure to pass the checks may result in the discontinuation of the negotiations, termination of the business relation or implementation of any mitigating measures if the Company deems this necessary.

5.3 Politically Exposed Persons

Situations involving PEP require the application of EDD measures, independently of the outcome of the risk assessment. This entails having to determine whether a counterparty is a PEP or otherwise and, should this be the case, apply of the following pre-established EDD measures:

- i. Obtain senior management approval to service the PEP;
- ii. Establish what is their source of wealth and, where applicable, their source of funds; and

Conduct enhanced on-going monitoring of the counter party's transaction related to the services provided by the counterparty

6. The Monitoring of Counterparty activities

The Managing director of the Company takes reasonable steps to prevent the activities of ML, TF and PF and monitors the usage of the services and related transactions

conducted by the Counterparty to detect any possible attempts for misuse of the platform through either the tampering with the provided software or any further requests.

6.1 Unusual activities

Any activities which are outside of the scope of the business relation, are not in line with the usual activities of the Counterparty and/or do not fit the normal business profile of a counterparty, require further investigation into the specifics of the case and might result in the submission of an unusual activity report to the Curaçao FIU where the activity gives rise of a suspicion of money laundering. Examples are:

Identity fraud

At the detection of any use of falsified documentation (identity fraud) of the Counterparty, the Company will proceed to conduct an in depth investigation. If the investigations confirm this fault, the Company will resolve to cancel/terminate the agreement with the Counterparty.

Refund requests

Refunding creates a legitimate paper trail between the Company and the Counterparty. Any business proposal or activity creating a credit which merits a refund is to be analyzed to prevent an unnecessary creation of the refund of an excess amount, thereby possibly aiding in the layering of ML by creating a legitimate financial transaction originated by the Company. The following activities should be thoroughly reviewed:

- Overcalculation of usage. Intentional overcalculation of the required usage of a product followed by a refund request for the non-use;
- Overpayment. The intentional overpayment followed by a request for a refund
- Unnecessary upgrades/ changes in the product portfolio followed by a request for refunding for the unused products.

7. Reporting of unusual transactions

Any unusual transactions or circumstances for which the Company has not received sufficient explanation may give rise to its report to the Curaçao FIU. The Company will hold a list of all instances in which it did not consider it necessary to report to the relevant authority. The decision not to report will need to be sufficiently supported. It is prohibited to inform the Counterparty or related third parties, of the reporting of or the intention to report an activity or transaction to the FIU.

8. Compliance officer (CO)

The Company may designate an CO who is in charge of the review of KYC information and transaction activities of the Counterparty. The CO would be further in charge of the following:

- i. identification and verification of the Counterparty striking an agreement with the Company
- ii. provide initial and ongoing training to all relevant staff
- iii. review of any unusual requests or activity by the Counterparty
- iv. Report Unusual transaction to the relevant authorities cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity; and
- v. ensure that this policy is adhered to, reviewed and maintained regularly.

9. Recordkeeping

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to

retain files in a way that enables investigating authorities to identify a satisfactory audit trail for transactions including the amounts, currencies and type of transactions.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

10. Periodical review of AML/CFT policies

The AML/CFT policies of the Company are subject to a yearly review, comprising of a fair and unbiased appraisal of each of the required elements of this policy. The review includes testing of internal controls and transactional systems and procedures to identify problems and weaknesses. The review may be conducted by an Employee or group of Employees, so long as the reviewer is not the CO and does not report directly to the CO.

Contact Information

For any questions regarding this policy, please contact:

eMoore N.V.
Legalcompliance Department
Groot Kwartierweg 10, Livestrong Building
Willemstad, Curaçao
Telephone: +599 9 7471401
Email: legalcompliance@the-emgroup.com