

Company - AML Procedure (Curacao)

Document information			
Document name:	Company - AML Procedure (Curacao)		
Document version:	1.1	Date of approval:	28.11.2024.
Approved by:	MLRO	Revision interval:	At least annually
Document owner:	Payments & Fraud Manager	Information classification:	Internal
Reference:	NA		
Revision history			
Author:	Version:	Date:	Change history:
Payments & Fraud Manager	1.1	28.11.2024.	Initial Version
COO	1.1	28.11.2024.	Approved Version
COO	1.2	02.06.2025	Updated Version

- [Introduction](#)
- [GEEKER TECHNOLOGY NV control framework](#)
- [What does this Policy cover?](#)
- [Who is responsible under this policy?](#)
- [Our approach to detecting, managing and preventing money laundering and terrorist financing](#)
- [What is money laundering, terrorist financing and proceeds of crime?](#)
 - [Money laundering](#)
 - [Terrorist financing](#)
 - [Proceeds of Crime](#)
- [Customer due diligence](#)
- [Transaction monitoring and suspicious activity reporting](#)
 - [Customers' Risk Assessment \("CRA"\)](#)
 - [GEEKER TECHNOLOGY NV's risk profiles](#)
 - [Risk profile model](#)
 - [Risk profile documentation](#)
- [Periodic systems monitoring](#)
- [External Suspicious Activity Reporting and working with the](#)
 - [Authorities](#)

- [Staff training](#)
- [Protection of employees and whistleblowing](#)
 - [Protection of employees](#)
 - [Whistleblowing](#)
- [Record keeping](#)
 - [Processing of personal data and documentation](#)
 - [Processing of special categories of personal data](#)
 - [Retention of documents and data](#)
 - [Prohibition of Disclosure \(Tipping Off and Professional Secrecy\)](#)
- [How we manage our risk of internal and external fraud](#)
- [How we manage our PEP and sanctions risk](#)

Introduction

Geeker Technology NV is a gambling operator licensed by the Curacao Gaming Authority. This is our policy to:

- conduct all of our business in an honest and ethical manner;
- prevent people engaged in money laundering, fraud, and other financial crimes, including terrorist financing, from using Geeker Technology NV services; and
- comply with all applicable laws and regulations covering money laundering, e-money/money transmission, payment processing, consumer protection and fraud, as prescribed by the Curacao Gaming Authority

We will meet this goal through all employees complying with the *GEEKER TECHNOLOGY NV* Policies and Procedures. GEEKER TECHNOLOGY NV will direct all necessary resources required to ensure that GEEKER TECHNOLOGY NV complies with the requirements and obligations set out in all applicable legislation, regulations, rules and industry guidance.

This AML Policy sets out the principles we follow to protect GEEKER TECHNOLOGY NV and its reputation from being misused for money laundering and/or terrorist financing or other illegal purposes. Its purpose is to:

- set out our responsibilities and those working for us, in observing and
- upholding our position on compliance; and
- explain where further detailed guidance can be found explaining how we apply this Policy in our day to day business operations.

Any failure to follow this Policy (and its associated Compliance Procedures) could severely harm GEEKER TECHNOLOGY NV's reputation, financial standing and possibly breach the terms of the licences necessary to operate our businesses. Such a failure may result in disciplinary action or termination for any employee found to have breached this Policy and may constitute a criminal offence. It should also be remembered that our compliance obligations include all our Policies and Procedures as well as those requirements that arise from the numerous contractual

relationships with card schemes, banks and other payment related partners that we have entered into in order to do business.

GEEKER TECHNOLOGY NV control framework

GEEKER TECHNOLOGY NV has in place, “three lines of defence” to protect against compliance breaches:

- our front-office, customer facing teams are responsible for identifying, assessing and controlling the risks relevant to our business. They have clear, written Policies and Procedures that set out GEEKER TECHNOLOGY NV’s expectations and processes that must be followed to ensure that we operate a sound system of control. This policy framework is set out in further detail below;
- we have appointed Money Laundering Reporting Officers as required for our business to ensure that we operate and maintain effective systems of control to manage our money laundering and terrorist financing risk and have implemented compliance controls to ensure compliance with applicable legislation.
- through our use of both
 - i) our internal audit team to independently evaluate our risk management and controls, reporting to the Audit Committee of GEEKER TECHNOLOGY NV; and
 - ii) external auditors.

What does this Policy cover?

This AML Policy applies to all GEEKER TECHNOLOGY NV staff (as set out in “Application of this Policy”). GEEKER TECHNOLOGY NV is committed to complying with all applicable regulations and licences held by our business and seeks to apply much of the regulated approach to all our businesses. This Policy is split into the following areas:

- our approach to detecting, managing and preventing money laundering and terrorist financing;
- what players we will accept;
- how we manage our risk of internal and external fraud;
- how we manage our politically exposed persons (PEP) and sanctions risk.

Who is responsible under this policy?

All of us within GEEKER TECHNOLOGY NV are required to comply with this AML Policy. Amendments to this Policy must be approved by the MLRO

Our approach to detecting, managing and preventing money laundering and terrorist financing

GEEKER TECHNOLOGY NV is committed to maintaining a robust anti-money laundering and antiterrorist financing programme – ensuring compliance with its responsibilities. As such GEEKER TECHNOLOGY NV will:

- not conduct business with any enterprise or person known or reasonably believed to be involved in narcotics trafficking, terrorism financing, money laundering or other criminal activities;
- comply fully with all applicable anti-money laundering and terrorism financing laws;
- ensure robust customer, affiliate due diligence processes are in place;
- monitor financial activities to identify reportable transactions and to assist in the detection of possible money laundering;
- never give advice or other assistance to customers or affiliates regarding how to structure transactions to evade reporting requirements or how to launder money; refuse to enter into or continue a transaction if it is known or suspected that the transaction is being conducted to avoid applicable reporting requirements or with the proceeds of criminal activity;
- refer suspicious activity promptly to the responsible MLRO to determine whether the activity may indicate known or suspected money laundering; and
- with the advice of the responsible MLRO, co-operate fully with law enforcement authorities.

What is money laundering, terrorist financing and proceeds of crime?

Money laundering

Money laundering is prohibited in the Curacao, in the European Union countries and other countries in which GEEKER TECHNOLOGY NV conducts business or has customers. Some countries impose reporting requirements and controls on financial and commercial transactions. Under these laws, it is a crime to engage knowingly in a commercial or financial transaction of any amount that is known or suspected to involve the proceeds of drug trafficking or other criminal activity.

Anti-money laundering enforcement authorities use reporting requirements to identify and pursue suspect transactions. Severe criminal and civil penalties may be imposed against companies and their officers, employees and customers for breaching the anti-money laundering rules and reporting requirements. The European Union requires all member states to pass laws making money laundering illegal and requires businesses in the financial sector to report instances of money laundering to the relevant local authorities.

Terrorist financing

There are very strict laws concerning terrorism. These are similar to the money laundering laws and create a number of main offences involving dealing with or possessing criminal property, or helping others to do so. It is important to note that “terrorist property” includes money or other property which is likely to be used for the purposes of terrorism, as well as proceeds of the commission of acts of terrorism or acts carried out for the purposes of terrorism.

Failure to report offences and tipping off offences also apply under the terrorism legislation. In practice, any circumstances that may indicate that any property or customer may be connected to terrorism, or any other information relating to terrorist offences, **must** be reported to the responsible MLRO immediately.

Traditionally, terrorist financing originates from a seemingly legitimate source. For example, organisations posing as charities and accepting donations may in fact use the proceeds to fund terrorist activity. In a regulated firm such as GEEKER TECHNOLOGY NV, senior management **must** ensure systems and controls are in place, to detect and prevent Money laundering/Terrorist Financing.

Proceeds of Crime

The illicit proceeds of any crime are considered criminal property. Money laundering offences can involve criminal conduct anywhere in the world.

Customer due diligence

It is important for us to know who the users of our products are so that we can:

- manage our financial risk and exposure to them appropriately; and
- fulfill our responsibilities to prevent money laundering, fraud and terrorist financing.

GEEKER TECHNOLOGY NV’s due diligence procedures deal with identifying users and understanding their expected product use and source of funds. Our user identification processes are split into:

- **customer** (individuals) due diligence processes

Due diligence **must** be carried out on **all** accounts to identify the identity of those who use our systems:

- when they apply to open an account with us or we start a business relationship with them;
- if we suspect them of involvement in money laundering or terrorist financing; or
- if we doubt any of the documents, data or information that they have previously provided to us.

Customer due diligence

As part of its commitment to responsible business, GEEKER TECHNOLOGY NV has adopted a risk-based approach to customer due diligence using a standard set of risk matrices to ensure that we take a consistent, risk-based approach to our customer identification and verification responsibilities and appropriately manage higher risk situations.

Unless a customer can satisfy our due diligence requirements, we will not open the account or continue business with that customer.

GEEKER TECHNOLOGY NV has defined three levels of customer due diligence for customers using the wallet:

- **Simplified Due Diligence (SDD)** – we collect identification information from every customer during the account opening process which at a minimum includes – name, address and date of birth. We also carry out PEP, sanction and adverse media screening on all applications for customer accounts
- **Full Due Diligence (FDD)** – Full due diligence is a means of verifying a customer's identity against government issued ID documents, documents, utility bills, bank statements and may also include the use of data brokers and webcam face match. Customers have the option to undergo Full Due Diligence in order to upgrade their account to allow withdrawals. For Additional information on our KYC process, please see KYC Verification Procedures; and
- **Enhanced Due Diligence (EDD)** – we apply EDD on a risk sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing as well as when certain thresholds are reached. The risk- based approach uses country risks, account thresholds and PEP status. EDD checks include account reviews, full review of transaction history, recording occupation and source of wealth, verification of source of wealth and requests for certified identification documents. Responsible MLRO approval and periodic account reviews are also required for any customers subject to EDD. For additional information on our EDD process, please see EDD Procedure

Transaction monitoring and suspicious activity reporting

After GEEKER TECHNOLOGY NV has entered into a business relationship with a user of our products, all transactions undertaken throughout the course of our relationship are monitored on an ongoing basis. This helps us ensure that the transactions are consistent with our expectations, given our knowledge of the user, their business and risk profile. It also allows us to identify any unusual patterns of behavior that may be indicative of illegal activity.

GEEKER TECHNOLOGY NV transaction monitoring is conducted on a risk-based approach under which the intensity of measures preventing money laundering and terrorist financing depend on the level and nature of the identified risks. Where a higher risk of money laundering or

terrorist financing is detected a more enhanced and focused approach is used and stricter thresholds, rules and measures are implemented.

Customers' Risk Assessment ("CRA")

The Customers' Risk Assessment is based on the findings of the conclusion of the Business Risk Assessment.

GEEKER TECHNOLOGY NV's risk profiles

In carrying out the risk assessment of customers, GEEKER TECHNOLOGY NV uses the following risk profiles:

- Low risk
- Medium risk
- High risk

Risk profile model

In accordance with the business risk assessment, the customers will be deemed to have a low risk profile, unless information revealed during the customer due diligence process or the ongoing monitoring of the customer relationships entails a different scoring. In these assessments, particular attention should be paid to circumstances which may indicate a high risk of money laundering as set out in Player Risk Matrix

Risk profile documentation

The customer's risk is based on the information that GEEKER TECHNOLOGY NV collects at the minimum of the EUR 2,000 threshold.

If we detect suspicious behavior, the account is reviewed by our staff to determine whether:

- we should continue to carry on business with this user; and/or
- whether Internal Suspicious Activity Report ("**Internal SAR**") needs to be filed with the responsible MLRO.

All employees **must**:

- read and commit to follow all the compliance requirements relevant to their business;
- ensure that all documents, data and information concerning users of our products is accurate and up to date;
- be familiar with internal escalation procedures for filing Internal SARs linked to money laundering or terrorist financing with the responsible MLRO;

- file an Internal SAR with the responsible MLRO following the when he/she has any of the following:

a) suspicions that an account is being used for money laundering, terrorist financing or other criminal activities; or

b) has reasonable grounds to suspect that any attempted, upcoming, ongoing or previously conducted transaction involving GEEKER TECHNOLOGY NV products may constitute criminal conduct or involve the proceeds or funding of criminal activity.

Failure to make, without reasonable excuse, a report about a suspicious transaction may constitute a criminal offence and represents a serious breach of an employee's contract of employment that may have disciplinary consequences.

It is also crime to "tip off" a suspected money launderer. This means that where any Internal or External SAR is made, you **must not** inform a customer or any other person that a SAR has been made or do anything that might prejudice any investigation the police or other authorities might carry out. "Tipping Off" is a criminal offence punishable by a term of imprisonment and/or a substantial financial penalty.

Business Risk Assessment

Geeker Technology NV performs an annual Business Risk Assessment (BRA), approved by the Board, to determine its ML/TF/FP risk appetite. The BRA methodology, factors assessed and results are retained for five years and provided to the GCB on request.

All business risk assessments are documented, stored as well as tracked with a description of the business or technology area. Quarterly these are reviewed by senior management team ahead of presentation of findings, priorities and recommendations to the board.

Before the launch of any new product, delivery channel or technology, the MLRO conducts and documents a Technological Developments Risk Assessment, identifying ML/TF vulnerabilities and mitigating controls.

Prevention of financing on weapons of mass destruction

Preventing the financing of weapons-of-mass-destruction (WMD) proliferation protects global security and directly supports international peace efforts. UN Security Council Resolutions require every country—and, by extension, every business operating within those jurisdictions—to curb financial flows that could help rogue states or non-state actors acquire nuclear, chemical, or biological weapons. Allowing such funding to slip through not only raises the threat of catastrophic humanitarian harm but also exposes the organisation to severe legal sanctions, loss of licences, and lasting reputational damage. By cutting off proliferation financing at the

source, we fulfil our regulatory duties, safeguard the integrity of the financial system, and do our part to reduce the risk of mass-casualty weapons falling into the wrong hands.

1 Customer / Beneficial-Owner profile

For all non-natural-person accounts we identify all natural persons owning $\geq 25\%$ or exercising ultimate control and verify them with reliable independent documents; where no natural person is identified the most senior managing official is treated as BO

- Provides vague or incomplete information on proposed activities or refuses supporting documents.
- Owners, directors or key staff appear on UN/EU/US sanctions or export-denial lists.
- Has nationality, residence or close business ties with a jurisdiction of proliferation concern (e.g., DPRK, Iran, Russia).
- Trades in dual-use or complex technical goods that do not match its stated business or expertise.
- Operates through shell/front companies with minimal capital or a mass-registration address.

2 Account & payment behaviour

- Originator or beneficiary bank is located in a PF-high-risk or weak export-control country.
- Circuitous payment chains (multiple hops, “ledger”/netting arrangements).
- Sudden cash deposits followed by withdrawals to purchase industrial or controlled goods.
- Personal accounts used to pay for commercial dual-use items.

3 Trade-related activity

- Freight forwarder or logistics firm listed as final consignee; importer differs from payment beneficiary.
- Invoices, contracts or customs forms show inconsistent quantities, values or end-users, or very low value relative to freight cost.
- Goods are technologically advanced for the destination country’s known industrial base.
- Third-party pays for shipment but is not named in trade paperwork.
- Shipments routed through multiple trans-shipment hubs or countries with weak sanctions enforcement.

4 Maritime / shipping clues

- Vessel exhibits frequent flag-hopping, AIS disablement or port calls that do not match the declared trade route.
- Exporter or importer registered at a PO-box or mass-registration address, or uses an opaque freight forwarder.

5 Financing tools & emerging methods

- Payments channelled through virtual-asset service providers (VASPs) or other alternative rails in PF-high-risk jurisdictions.

Alternative Dispute Resolution

- **Engage only CGA-certified ADR bodies.** Certification for ADR providers opened in June 2025; proof of the chosen provider's certificate will be retained on file.
- **Offer ADR free of charge to players once internal complaint handling is exhausted,** and ensure decisions are binding on the company when accepted by the customer.
- **File an ADR outcomes report to the CGA every quarter starting January 2026** (same cadence as the new player-complaints return).
- **Maintain a complaints & ADR register for five years** showing issue date, subject, sums in dispute, resolution date and outcome, ready for CGA inspection.
- **Monitor ADR trends** and feed lessons learned into the annual Business Risk Assessment and ongoing staff training.

Periodic systems monitoring

GEEKER TECHNOLOGY NV is committed to carrying out periodic reviews of the effectiveness of due diligence and screening processes. As part of the review a selection of user accounts are reviewed and rescreened and the findings reported to the responsible MLRO and assessment made of the controls processes. This is reported to the MLRO and to the Audit Committee.

External Suspicious Activity Reporting and working with the

Authorities

GEEKER TECHNOLOGY NV is committed to identifying and reporting any suspicious activity that may be linked to money laundering or terrorist financing. As part of our commitment to responsible business, we will:

- Report any activity to the FIU authority including providing them with any relevant documentation
- support the relevant authorities in their lawful investigation of suspicious activities; and

- use the information provided by those authorities in our risk assessment and management of our business.

GEEKER TECHNOLOGY NV will support the responsible MLRO to fulfill their responsibility to ensure that all Internal SARs are promptly investigated and, if appropriate, notification made to the relevant authorities.

Staff training

A key element of our compliance programme is ensuring that all employees are trained as to their compliance responsibility and developments in the area. Training includes how to identify reportable situations and other signs of money laundering and terrorist financing, what roles management and the MLROs and other officers and employees have within GEEKER TECHNOLOGY NV compliance activities, how to perform such duties and responsibilities and what to do once an employee believes that a reportable situation has arisen or suspicious activity has been detected. This sets out our commitment to train staff:

- when they join GEEKER TECHNOLOGY NV;
- at least annually for refresher training; and
- when requested or as the need arises due to significant development.

The level of training received by the staff is determined by their role within GEEKER TECHNOLOGY NV.

All GEEKER TECHNOLOGY NV staff **must** take part in the mandatory training assigned to them. Failure to do so without good reason constitutes a significant breach of their employment contract and may result in termination of their employment.

The training is documented, electronically or in paper form, with the following information:

- Content of the training
- Name of the participants
- Details of the trainer
- Date of the training

GEEKER TECHNOLOGY NV conducts training either on a face-to-face basis or via electronic means, depending on the location of the participants.

Protection of employees and whistleblowing

Protection of employees

GEEKER TECHNOLOGY NV has established routines to protect persons who fulfil the GEEKER TECHNOLOGY NV 's obligations under the Curacao Prevention of Money Laundering Act. Further information can be found in Employee Protection Procedures.

Moreover, any individual (including employees, consultants and GEEKER TECHNOLOGY NV official) who reports suspicions of ML/TF, internally or to the FIU, is protected under the regulations from threats or hostile action, and in particular from adverse or discriminatory employment actions. Further information can be found in Whistle Blowing Procedure

Whistleblowing

The GEEKER TECHNOLOGY NV has established a whistleblowing system under which internal violations of the Curacao Prevention of Money Laundering Act or these guidelines can be reported anonymously and without risk or reprisal. Further information can be found Whistle Blowing Procedure

Record keeping

All documents, data and other information concerning customer, merchant or distributor identification and transactions **must** be kept and held in accordance with the *Global Assets & Financial Integrity: Document and Data Retention Procedure*.

The contents of all investigations and reporting on PEPs and sanctioned individual **must** remain confidential to the responsible MLRO.

Processing of personal data and documentation

Processing of special categories of personal data

Special categories of personal data in the meaning of Article 9.1 of Regulation (EU) 2016/679 ("GDPR") may be processed if necessary, to:

- (a) Assess if the customer is a PEP or family member or a person known to be a close associate to a PEP.
- (b) Assess the customer's risk profile.
- (c) Assess suspicious transactions/activities and comply with the monitoring obligation as per section 5 above.
- (d) Provide information to the Police in accordance with these guidelines and answer questions from the Police regarding money laundering.

(e) Retain documents and data if it is permitted to process them in accordance with (a)-(d).

Personal data referred to in Article 10 of the GDPR (relating to criminal convictions and offences) may be processed under the conditions set out in points (b)-(e) above.

Retention of documents and data

GEEKER TECHNOLOGY NV retains for five years, from the end of the business relationship, documents and data to the extent it concerns:

- Customer due diligence.
- Transactions subject to customer due diligence requirements.

The GEEKER TECHNOLOGY NV retains documents and data for ten years, when:

- The documents or information indicate ML/FT or that property otherwise derives from criminal activity, and
- This has been reported to the relevant Financial Intelligence Unit ("FIU"), in accordance with Section 5.2 of these guidelines, and
- An authority has informed GEEKER TECHNOLOGY NV that such documents or data need to be retained for a longer period of time.

The retention period is calculated from the performance of the measures/transactions or where a business relationship has been established, the relationship was terminated. If a single transaction has not been executed as a result of suspicion of money laundering, the retention period is calculated from the time the decision was made not to execute it.

The documents/data is dated and stored safely, electronically or in paper form, and be easy to identify, obtain and compile.

Prohibition of Disclosure (Tipping Off and Professional Secrecy)

The fact that personal data is processed for investigating suspicions of ML/FT, or for a ML/FT report to be compiled, or for contacts or correspondence on ML/FT with the relevant FIU, or that data is processed or retained in accordance with this policy, such data may not be unlawfully disclosed to the data subject or another third party. Therefore, confidentiality applies to such personal data processing.

If any employee/official discloses to the person concerned or to a third party that an analysis is being carried out or that information has been transmitted to the relevant FIU, or that the relevant FIU has transmitted the information to the police for investigation, such individual is guilty of an offence and liable on conviction.

A disclosure is not unlawful if it means that information is provided to a supervisory authority or a law enforcement agency in a disciplinary matter or other matter that justifies the provision of such information,

How we manage our risk of internal and external fraud

GEEKER TECHNOLOGY NV is committed to maintaining strict standards of honesty as an essential part of all its stakeholders' interests, whether they are shareholders, employees or customers. We are committed to developing, implementing and maintaining controls to reduce fraud to such levels as are acceptable given its significant impact on business reputation, shareholders, customers, third parties and staff.

As such, it is our policy to:

- take action against any employee committing or assisting fraud against GEEKER TECHNOLOGY NV, our employees or our customers.
- ensure active recovery of funds lost due to fraud using all available legal means where appropriate.

We have in place a confidential mechanism to report internal concerns related to financial crime.

If you know of, or suspect breaches of the GEEKER TECHNOLOGY NV's Policies and Procedures, you must report it in accordance with Whistle Blowing Procedure This Procedure aims to protect those who speak up about possible or actual breaches and ensure that concerns are subject to an appropriate investigation. GEEKER TECHNOLOGY NV will not tolerate the victimization of anyone who speaks up.

How we manage our PEP and sanctions risk

For every VTML account, we will check (using a screening solution provided by a third party) against the following:

- **Global Politically Exposed Persons (PEPs)** and their associates or family members.
- **Office of Foreign Assets Control (OFAC) Sanctions:** OFAC administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign states, organisations, and individuals. The OFAC lists include the Specially Designated Nationals (SDN) List, United Kingdom Sanctions Act lists, and EU Consolidated Sanctions List.
- **The Financial Action Task Force (FATF) Guidance:** The FATF is an intergovernmental body whose aims are to set standards and promote 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.

Further checks **must** be made as set out in the risk matrices and whenever the lists or database are updated.

Before we enter into a business relationship with a PEP (or continue a relationship), prior written approval from the responsible MLRO **must** be received.

If there is a confirmed match to a sanctions list entry then the business relationship **must** be promptly terminated, a notification to the responsible MLRO made as well as a report to the relevant authorities where applicable.

Confirmed matches to the PEP database will be subject to enhanced monitoring and the business relationship will require approval from the responsible MLRO to continue.

Date: __28.11.2024.____

For GEEKER TECHNOLOGY NV

Oliver De Bono
