

AML & CFT Policy

Novatech Solutions N.V

Version 1.4

Document Status

Version Number	V1.4
Status	Active
Authorisation and approved by	The directors of Novatech Solutions N.V. on 23rd January 2025.
Review	On or before February 2026
Owner	Merissa Tampal - MLRO
Number of pages	12 Pages

Version Control

Effective date	Version	Comments	Author
August 28th 2021	1.0	Policy creation	Joanna Arenas
October 23rd 2022	1.1	Minor changes	Joanna Arenas
March 13th 2023	1.2	Annual review	Joanna Arenas
May 28th 2024	1.3	Policy amendments	Merissa T.
January 23rd 2024	1.4	Annual Review	Merissa T.

Sign off list:

Name	Position
Merissa Tampal	Compliance Officer - MLRO
Joanna Arenas	Director of Novatech Solutions N.V

Copyright

This document Is produced by Novatech Solutions N.V., exclusively for internal use. It contains confidential information; under no circumstances should it be delivered or disclosed to any person not employed by Novatech Solutions N.V. without the express written permission.

Contents

Document Status	2
Version Control	2
Novatech Solutions N.V - AML FRAMEWORK.....	4
Money Laundering (ML) and Funding Terrorism (FT).....	4
AML & CFT Programme	5
Risk Appetite	6
MONEY LAUNDERING REPORTING OFFICER (MLRO).....	6
Consideration of a disclosure by the MLRO	8
Politically Exposed Persons (PEP)	8
Customer Due Diligence - CDD	9
ONGOING CUSTOMER DUE DILIGENCE	10
Sanctions Programme.....	10
Data Protection and Retention	11
Internal and External Disclosures	11
Training Program	12

Novatech Solutions N.V - AML FRAMEWORK

The AML & CFT (Anti-Money Laundering & Countering the Financing of Terrorism) framework of Novatech Solutions N.V. (hereinafter "Company") is based both on international AML regulations of as well as on national legislation of Curacao:

- FAFT Recommendations,
- The National ordinance on the identification when rendering services
- The National Ordinance on the Reporting of Unusual transactions
- Sanctions National Ordinance
- The Code of criminal law
- Kingdom Sanction Act
- GCB Guidelines

The AML & CFT Policy outlines all matters related to the regulatory framework and provides a general overview of Novatech's defense against money laundering and terrorist financing.

This Policy shows how the statutory and regulatory obligations to prevent money laundering are to be met in full and the company is committed to meeting and where possible exceeding such obligations.

Money Laundering (ML) and Funding Terrorism (FT)

Type text here

Money Laundering describes the process by which a criminal may attempt to disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have been derived from a legitimate source.

The term 'proceeds of crime' refer to any money or property which a person obtains (directly or indirectly) as a result of criminal activities (e.g., money from drug dealing, or stolen in a burglary or robbery, or stolen from an employer, or obtained through some fraudulent scheme or by any other form of 'ill-gotten gains').

If the person uses that money to acquire other assets, then those other assets are also the 'proceeds of crime' (e.g., if a person uses money earned from drug dealing to buy a car or a house, or spends money gained in a bank robbery to gamble, it must still be considering to be the 'proceeds of crime').

Money laundering by a customer occurs either:

- Where the customer tries to spend the proceeds of crime on gambling (known as 'criminal spend').
- Where a customer uses our services to try to disguise the source of their money (i.e., 'classic' money laundering whereby a criminal tries to turn their ill-gotten gains in to 'clean' money by 'layering' it through a series of otherwise respectable transactions, so that they appear to have derived their wealth from legitimate activities).

This is the process of making funds or other assets available to support, even indirectly, terrorist activities. Indirect support provided to terrorists may take various forms, such as financial compensation, training, propaganda or even assistance related to living expenses.

ML and FT are separate crimes, and key distinctions exist between the two. Some of the core differences between ML and FT are:

Funds used for ML are derived from criminal activities, while the source of terrorist funds may originate from legitimate and/or illegitimate sources.

Concealment of funds to be used for terrorism or by terrorists is designed primarily to hide their identity or the purpose for which these funds are used. In ML, the funds are proceeds of illegal activity, and the primary purpose of the laundering is to conceal their source and enable the funds to be used legally.

AML & CFT Programme

To facilitate compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) laws, the Company has developed and implemented an AML and CFT framework consisting of policy, procedures, internal systems and controls. Company's AML and CFT programs include, but are not limited to:

- Appointment of a Money Laundering Reporting Officer (MLRO), who has a sufficient level of seniority and independence, to ensure compliance with the relevant legislation, regulations, rules and industry guidance. The MLRO is responsible for the day-to-day supervision and oversight of Company's and Business Unit compliance with relevant legislation, regulations, rules and industry guidance.
- Establishment and maintenance of a risk-based approach (RBA) to the identification, assessment, control and management of money laundering and terrorist financing risks facing the business.
- Risk-based customer due diligence (CDD)
- Customer Risk Assessment (CRA)
- Customer Acceptance Policy (CAP)
- Identification and assessment of politically exposed persons (PEP's)
- Establishment and maintenance of systems and procedures for the monitoring of customer activity
- Establishment and maintenance of internal procedures for reporting suspicious activity to the nominated officer and ensuring effective investigation with escalation to the relevant law enforcement authorities as appropriate.
- Allocation of sufficient resource for the anti-money laundering programme to be effective.
- Maintenance and storage of appropriate records for the minimum prescribed periods.
- Establishment and maintenance of a sanctions programme to ensure screening for individuals on sanctions list(s) and to have procedures, in line with regulation, to close and report to the relevant regulatory body.
- Provision of transparency and visibility of key risks, activities and trend reporting to Group Compliance Committee, Operating Boards and other identified stakeholders.
- Regular training and awareness for all relevant employees; and
- Timely notification and reporting to the senior management upon Company's compliance with AML/CFT requirements.

Risk Appetite

All employees are expected to maintain high ethical standards and conduct their business practices in line with this Policy; and to act with due skill, care diligence and integrity.

There is no appetite for legal or regulatory breaches.

There is no appetite for deliberate misconduct by employees or third parties appointed by Company to perform any support services to the business.

MONEY LAUNDERING REPORTING OFFICER (MLRO)

The Company appointed the experienced MLRO whose effective influence can be exercised on the subject person's AML/CFT measures, policies, controls and procedures and should not be precluded from posing an effective challenge when necessary.

Additionally, the MLRO acts independently in carrying out his responsibilities and has full access to all the records.

The core functions of the MLRO are to:

- a) receive reports from Company's employees regarding customer unusual transactions, or through software solutions used to analyze transactions, on information or matters that may give rise to knowledge or suspicion of ML/FT, or that a person may have been, is or may be connected with ML/FT.
- b) Examine the above-mentioned reports in order to determine whether knowledge or suspicion of ML/FT exists or whether a person may have been, is or may be connected with ML/FT.
- c) report knowledge or suspicion of ML/FT or of a person's connection with ML/FT
- d) respond promptly to any request for additional for information from relevant bodies.

The MLRO is responsible for:

- Developing necessary policies, procedures, training and education of staff
- design and implementation of AML program;
- verification of the adherence to the local legislation and regulations regarding detention and deterrence of ML/FT;
- periodic revision of this Policy and other framework;
- constant training and education of the Company's employees (no rare than once in 12 months);
- analysis of the transactions with further reporting thereof to the relevant enforcing agencies (if necessary);

- revision of all internally reported to the senior management of the Company suspicious transactions and/or unusual activity of the customers;
- records keeping of internally and externally reported unusual transactions;
- execution of the closer investigations of unusual transactions;
- preparation and submitting of the external report of unusual transactions to the enforcing agencies;
- necessary changes to AML program;
- constant acknowledgement of any changes o international and local ML/TF and suggestions made upon improvements to the senior management;
- periodic informational review upon the Company's efforts regarding combat of ML/FT.

The MLRO maintains a register separately from other records associated with the company which details:

- Enquiries made to the company Solutions N.V by law enforcement or other officials acting under powers provided by the Money Laundering and Terrorist Financing Requirements.

This External request register contains:

- The nature and date of the enquiry
- The name of the enquiring officer and enforcement agency
- The powers being exercised
- Details of the player
- Details of the transaction
- Outcome of enquiry (if known)

All reports made to the MLRO by the Company employees are keep in a register that contains:

- The nature and date of the report including details of the player.
- The name of the person making the report.
- Information about the transaction which is sufficient to identify the relevant Beneficiaries.
- Details of the acknowledgement of receipt of report provided by the MLRO.
- Relevant red flags.
- Outcome of the report

MLRO Contact details:

Merissa Tampal

met@novatechnv.com

Consideration of a disclosure by the MLRO

Upon receiving a disclosure, the MLRO will evaluate the report promptly to:

- Determine if there is knowledge or suspicion of money laundering.
- Assess if there are reasonable grounds to know or suspect money laundering.
- Determine whether a Suspicious Activity Report (SAR) must be filed.

If the MLRO determines that there are no reasonable grounds to suspect money laundering, the MLRO will document the rationale for this decision in the internal records.

In situations where there is suspicion of money laundering and/or terrorist financing, the Company may proceed with a transaction only if ceasing the transaction is impossible or would hinder an ongoing investigation. This decision must be carefully documented and justified by the MLRO.

The MLRO must also consider the need for additional notifications and reports to the Financial Intelligence Unit (FIU) whenever concerns, suspicions, or grounds related to money laundering and terrorist financing arise.

Politically Exposed Persons (PEP)

A Politically Exposed Person (PEP) is an individual who is or has been entrusted with a prominent public function, as defined by the Financial Action Task Force (FATF). This includes individuals holding prominent positions in government, state-owned enterprises, international organizations, and their close family members and associates.

PEPs present a higher risk of money laundering and terrorist financing due to their positions and influence, which may be misused for personal gain through activities such as bribery, corruption, and misappropriation of funds. Family members and close associates of PEPs also pose a higher risk, as they may benefit from or facilitate the PEP's abuse of power.

PEP screening is conducted before at the start of the business relationship and on an ongoing basis. The Company utilizes LexisNexis for PEP screening. Regular screening is conducted because a customer's PEP status may change over time.

If a potential PEP match is identified, the AML team will investigate to confirm the match. True matches will be reported to the MLRO, who will:

- Conduct enhanced ongoing monitoring of the relationship.
- Obtain senior management approval for establishing or continuing the business relationship.
- Take reasonable measures to establish the source of wealth and source of funds.
- Once a True match is detected, additional the following measures will be applied: Conduct Enhanced ongoing monitoring
- Obtain senior management approval for stablish the business relationship for new customers or continuing the business relationships for existing customers.
- Take reasonable measures to stablish the source of wealth and the source of funds.

Customer Due Diligence - CDD

The Company is committed to conduct customer due diligence (CDD) measures in accordance with all applicable laws and regulations. This includes performing Know Your Customer (KYC) checks on all customers and Enhanced Due Diligence (EDD) on high-risk customers.

The purpose of our KYC processes is to:

- Verify the customer's identity and age.
- Identify the beneficial owner(s) of the account.
- Ensure that the individual using the account is the registered customer.

The Company collects the following information from customers upon registration:

- First Name
- Last Name
- Street Address
- City
- Country
- Postal Code
- Date of Birth (must be 18 years or older)
- Email Address
- Contact Number

The Company takes all necessary measures to protect the privacy and security of customer data.

For customers classified as medium or high risk according to The Company's risk assessment procedures, the following additional information will be collected:

- Place of Birth
- Nationality
- Identity Number

Enhanced Due Diligence (EDD) measures will be conducted when a customer's profile or activity triggers a risk indicator, as determined by Company's risk assessment procedures, or if required by a regulatory or law enforcement agency.

ONGOING CUSTOMER DUE DILIGENCE

The Company maintain a robust ongoing monitoring program and scrutinize all the customers transactions. To maintain a robust ongoing monitoring process, the Company has implemented various financial and non-financial triggers, including behavioral ones, to effectively detect and mitigate ML/TF risks.

If a customer triggers an AML alert, a dedicated team will conduct a customer due diligence (CDD) review, the extent of which will depend on the customer's risk level.

- For low-risk customers a simplified due diligence will be carried out. If some red flags are encountered the risk level will be increased according to the outcome and information will be requested based on the outcome.
- For medium risk customers a smart assessment is conducted, minimum will include:
 - KYC information and Documentation.
 - Payment methods used.
 - IP history check.
 - 3rd party check.
 - Activity check.
 - PEP and Sanctions checks.
 - Occupation and SOF/SOW information
 - Ongoing monitoring
 - Escalation of the ML/FT suspicions or concerns.
- For high-risk customers, smart assessment is conducted and if the outcome shows player with different red flags, Enhance Due Diligence will be fully performed, including Enhanced ongoing monitoring.
- For those players such as confirmer PEP or customer that poses a very high-risk profile additional measures will be applied such as:
 - Senior management approval.
 - Enhanced ongoing monitoring.
 - SOW & SOF documentation
 - A case file will be complete on those customers that pose some ML & FT concerns.
 - ML/FT suspicions or concerns will be disclosed to the MLRO.

Sanctions Programme

Company utilizes LexisNexis, a third-party provider, to conduct sanctions screening for customers seeking to establish a business relationship. Sanctions lists screened include, but are not limited to, those maintained by the EU, OFAC, and UN.

Upon identification of a customer match on any sanctions list, the case will be immediately escalated to the MLRO. The account in question will be frozen, and all funds will be restricted from leaving the company's platform.

The MLRO will adhere to established procedures for notifying the relevant authorities of the sanctions match.

Data Protection and Retention

Records will be maintained in a secure and accessible form: Secure backups of all data are made on a daily basis and held at a location which shall be determined as soon as is reasonably practicable.

Records include:

- all registration details.
- identification verification
- enhanced due diligence.
- suspended accounts and reason for suspension.
- closed accounts.
- suspicious transaction reports
- financial transactions – deposits, bets made, withdrawals, prize payments.
- self-exclusions
- self-imposed limits
- excluded players.
- bets placed.
- complaints and responses
- audit trails
- accounting and bookkeeping records including VAT returns, duties payable etc.
- bank reconciliations
- Customer Service electronic correspondence records

Records associated with a player (including all identification records and the financial transactions made by them) are maintained for a period of 5 years after the date of closure of the player's account or the date of the last transaction.

Internal and External Disclosures

All Company's employees must follow up the escalation process described in the AML & CFT Procedures to disclose those cases that pose concerns or suspicions of ML/FT.

The Company maintains a log of all the disclosures made to the MLRO and disclosures made by the FIU.

The log it is divided into:

- Internal disclosure - any type of internal disclosure made to the MLRO (or deputy).
- External disclosure - ML/FT/PF disclosures made to the FIU.
- Other disclosures made to the FIU – Sanctions reporting or any other reports of any FIU.

As minimum the log will record the following:

- Action taken regarding any internal disclosures.
- Time elapsed between the internal disclosure being made and decision taken.
- Brief reason for suspicion (Re. external disclosures) or rationale for report (other disclosures). Ideally, this would be from a standardized list, in order to facilitate easy analysis.

Training Program

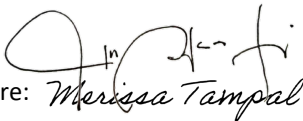
The Company ensures that employees regardless of the position attend, at least yearly, training in the recognition and handling of operations or transactions which may be related to proceeds of criminal activity or ML/FT.

The training can be conducted online, live session or through external platforms or courses.

All new employees will attend an induction to AML in which it is explained the basics of AML and CFT and the procedures to follow in the company. This initial training will be conducted in the following 30 days since the employee joined the company.

The Company maintains records of all the training conducted these records include:

- Details on content of training
- Names of the attendees.
- Date training was provided
- Results of testing carried out, if any.
- Ongoing training plan.

MLRO Signature: 

Date: 23/01/2025

Novatech's Director Signature: 

Type text here

Date: 23/01/2025

AML & CFT Policy V1.4 - Novatech Solutions N.V (2)

Final Audit Report

2025-01-23

Created:	2025-01-23
By:	Legal Dept (legal@novatechnv.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAmVU038JKOU0WpmuxFPMuGeHp6z_8nGAf

"AML & CFT Policy V1.4 - Novatech Solutions N.V (2)" History

-  Document created by Legal Dept (legal@novatechnv.com)
2025-01-23 - 9:37:27 AM GMT
-  Document emailed to joanna@novatechnv.com for signature
2025-01-23 - 9:37:32 AM GMT
-  Email viewed by joanna@novatechnv.com
2025-01-23 - 2:45:09 PM GMT
-  Signer joanna@novatechnv.com entered name at signing as Joanna T. Arenas
2025-01-23 - 2:47:56 PM GMT
-  Document e-signed by Joanna T. Arenas (joanna@novatechnv.com)
Signature Date: 2025-01-23 - 2:47:58 PM GMT - Time Source: server
-  Agreement completed.
2025-01-23 - 2:47:58 PM GMT