

Trenta Tech Group

AML Policy

Version	Date	Authorised by	Signature
V1.0	01/07/2021	Director	
V1.1	01/06/2022	Director	
V2.0	24/06/2023	Director	
V3.0	31/07/2024	Director	
V4.0	30/05/2025	Director	
V5.0	06/06/2025	Director	

Contents

1. Introduction	3
General Obligations	3
1. Regulatory Framework	3
2. Purpose and Scope	4
3. Definition of Money Laundering and Terrorist Financing	4
4. Business Risk Assessment	4
5. Customer Acceptance Policy	5
6. Required Customer Information (SDD)	5
7. Customer Due Diligence (CDD)	5
8. Reliance on third parties to perform customer due diligence	6
9. Obtaining Information on the purpose and intended Nature of the Business Relationship	7
10. Enhanced Due Diligence	7
11. Ongoing Monitoring	7
12. Enhanced Ongoing Monitoring	8
13. Internal Controls	8
14. Counter-Terrorist Financing	9
15. Politically Exposed Person	9
16. Known Criminals	10
17. Suspicious Transaction Reporting (STR)	10
18. High-Risk Jurisdictions	11
19. Training	11
20. Record Keeping	11
21. Employee Vetting	11
22. Policy Distribution	12
23. Due Diligence for Third Parties	12
24. Policy URL	12
25. Compliance and Consequences of Non-Compliance	12
Appendix 1:	13
Appendix 2:	14

1. Introduction

This document outlines the Group AML policy of Trenta Tech Group, including the entities of Trenta Tech Ltd and its subsidiary Niollo BV (The Group). Trenta Tech Limited contractually manages customer operations on behalf of Niollo BV and thus must ensure that when handling Niollo BV's customers that the requirements of the Curacao Money Laundering Legislation¹ are followed, and the business has policies and procedures to aid compliance with that. The main scope of this policy is to establish the essential standards designed to prevent Trenta Tech Ltd or Niollo BV from being used for money laundering and terrorism financing. This policy sets out the procedures that must be followed to enable The Group to comply with its legal obligations. To give effect to this AML policy, the group is committed to:

- (i) Formulate and implement internal rules and develop procedures and systems to detect and monitor suspicious transactions and to report thereon to the relevant authorities.
- (ii) Ensure sufficient resources are devoted to the training of staff, increase their awareness and ability to deal with suspicious transactions and to keep them informed of new legislative developments and requirements.
- (iii) Ensure commercial considerations never override the need to comply with the Regulations.
- (iv) Create an environment where staff who report on suspicious transactions can do so confidentially and without fear of reprisal.

General Obligations

- i. This Anti-Money Laundering (AML) policy applies to The Group and all of its staff who provide services which might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.
- ii. The Group is required to have adequate policies, procedures, and controls that identify, assess, and mitigate the risk of Money Laundering/Terrorist Financing. This is fulfilled by having:
 - Policies and procedures that are compliant to the regulatory requirements
 - Business and Customer Risk Assessment Practices and Procedures
 - Know your customer (KYC) policies and procedures
 - An internal and external Suspicious Activity Reporting (SAR) system
 - AML Training to all relevant staff at least annually
 - Appropriate record keeping in relation to AML
- iii. Having a robust ML/TF Risk management framework is implemented in order to prevent, detect, and report on suspicious transactions.

1. Regulatory Framework

Below is a list of all the relevant AML legislation and regulations pertaining:

- Curacao Gaming Board Regulations for AML/CFT
- National Ordinance on Identification when rendering services (N.G 2017, no 92)
- NORUT – National Ordinance on the Reporting of Unusual Transactions (N,G 2017, no 99)

¹ For copies of the Act and Regulations, access the Ministry of Justice site at: <https://www.gamingcontrolcuracao.org/regulation/aml>
TRENTA TECH GROUP AML & CTF POLICY V2.0

- Sanctions National Ordinance (N,G 2014, no 55)
- Kingdom Sanction Act (N,G 2016, no 54)
- National Decree entering into force of Kingdom Sanction Law (N.G 2017, no 2)
- The Code of Criminal Law (Penal Code) N.G 2011, no 48)
- National Ordinance on Games of Chance (LOK)

2. Purpose and Scope

The Group is mandated by the AML directives, as well as National Legislation and Regulations, to identify persons potentially carrying higher risk in order to prevent any misuse of its sites for criminal purposes. This procedure applies for all customers falling under the Curacao licence of Niollo and business to business relationships Trenta Tech has.

3. Definition of Money Laundering and Terrorist Financing

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction, and confiscation of the criminal funds. There are three stages in the process:

- I. Placement: Illicitly obtained money first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments.
- II. Layering: How the link between the funds and the criminal is concealed.
- III. Integration: Investing and/or recovering the funds in a way that looks legitimate.

Terrorist financing involves the solicitation, collection, or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources.

4. Business Risk Assessment

The business must conduct a Business Risk Assessment (BRA) at the outset, covering four areas

1. Customer Risk
2. Geographical Risk
3. Product/Service and Transaction Risk
4. Distribution Channel Risk

The BRA must be reviewed at least once annually or when any major change in the above risk categories occur such as a new product addition or added payment method type to the offer.

The BRA must:

- Identify AML-related risks that the business is exposed to
- Design and implement policies and procedures to manage and mitigate these assessed risks.
- Monitor and improve the effective operation of these controls; and
- Record what has been done, and why.

The BRA must be approved by the company directors and MLRO.

5. Customer Acceptance Policy

The business must have a customer acceptance policy outlining:

1. A description of the type of players that are likely to pose a higher-than-average risk of ML/FT/FP.
2. The risk indicators present low, medium, or high risk.
3. The level of Customer Due Diligence (CDD) measures, including ongoing monitoring to be applied.
4. The circumstances under which service to someone is declined.
5. Politically Exposed Persons (PEP) and Sanctions Screening checks and policy

6. Required Customer Information (SDD)

In order to help prevent money laundering and terrorist financing, The Group performs KYC on its customers.

The Group KYC procedures require prospective customers to create a full profile at the point of registration. The mandatory information required at the registration (SDD) stage includes:

- True Name and Surname
- Residential address
- Country of residence
- Date of Birth
- Password
- Unique Phone Number & email address

7. Customer Due Diligence (CDD)

By following a risk-based approach, the appropriate due diligence (CDD) can be applied to a customer. This means that the higher the ML/FT risk is, the greater the level of due diligence will be applied. The Group identifies and performs verification checks on all players, as set out by the applicable regulations for the entity. Verification may be carried out before the customer reaches thresholds if suspicious activity is detected.

Stronger than the Curacao regulations, requiring customer due diligence to be requested upon a customer reaching total lifetime deposits or withdrawals of 4000NAF/200USD, the Group requests due diligence when cumulative deposits reach 500 USD or when any withdrawal is made, unless customer due diligence has been performed already due to heightened suspicion.

No customer may withdraw at any time until they have completed CDD. Once a customer reaches deposits of 4000NAF/2000USD then no further deposits are allowed until the customer passes the CDD checks.

Customers have 30 days to pass such checks in the event of suspicious activity or once exceeding the 4000NAF/2000USD threshold else are closed.

Customer Due Diligence Documentation

TRENTA TECH GROUP AML & CTF POLICY V2.0

In order to verify the details on their player account, our Group requests the customer to provide a copy of one document from each of the categories listed below:

Personal information

- Valid Passport
- Valid Driving License
- Valid National Identification Document (Picture ID)

The Group may accept other types of identity documents that are in line with Curacao regulatory requirements.

Expired ID documents are not permitted, except ID documents older than 6 months from issue are not permitted. IDs that expire after CDD has been completed can be re-requested on a risk-sensitive nature based on the activity of the account.

Liveness Checks

The group also perform liveness checks on all customers passing through due diligence to confirm the person supplying the photo identity is who they say they are. The images from photo identity are checked against the identity card for match using AI and further against the whole database of photos for duplicate accounts.

Address Information

Where the identity document does not allow verification of one's residential address, the following documents will be requested:

- Utility Bill, which is less than 3 months old. Mobile phone bills are not sufficient. The bill provided must pertain to a service delivered to the address provided
- Valid Driving License Tax Bill, which is less than 6 months old
- A copy of a Bank statement, which is less than 6 months old

Please see our KYC Procedures for a full list of acceptable documents.

Source of Payment Verification

In the event we need to verify a payment method, the customer will be required to provide:

- Registered Credit or Debit (Front and back)
- Account statement of payment registered with the account.

All documents received are vetted by employees and authenticity checks ensure the documentation is genuine and have not been tampered or are fake.

8. Reliance on third parties to perform customer due diligence

The Group does not rely on third parties to perform CDD measures in line with the Curacao regulatory requirements, laws, and regulations.

9. Obtaining Information on the purpose and intended Nature of the Business Relationship

The Group will request the collect sufficient information to allow the detection of unusual activity in the course of a business relationship.

The company will either use Central statistical data to gauge the customer's activity or collect from the customer their nature of employment/business and usual annual salary upon reaching total deposits of 4000NAF/2000USD.

Upon request for information, the business relationship will be terminated, 30 days from the initial request to provide this information.

When the risk of ML/FT is higher or casinos have doubts as to the veracity of the information collected, the customer will be required to provide enhanced due diligence documentation.

10. Enhanced Due Diligence

The Group may initiate enhanced due diligence documentation as part of any account review, if a customer is classified as high risk by the customer risk model (see business risk assessment) or when suspicions are raised that a customer is suspected of Money Laundering.

Enhance due diligence documentation may be requested upon a customer being identified as a politically exposed person. In all cases the business does not accept business from confirmed PEPs and any activity from the PEP will be refunded/voided.

When enhanced due diligence has been requested, the customer will be required to provide the following documentation:

Acceptable enhanced due diligence documentation

- Payslips
- Bank Statement showing Salary being received
- Tax Return
- Savings
- Company Financials

The Group may accept other types of documentation to satisfy that the funds used to gamble have come from legitimate sources. Please see the KYC Process documents for a full list of acceptable documents.

11. Ongoing Monitoring

The group must monitor transactions and use exception reporting to identify which be related to money laundering and terrorist financing. Each risk identified in the BRA must have an associated control.

Daily reports are received to monitor and identify unusual patterns. All reports are handled by the
TRENTA TECH GROUP AML & CTF POLICY V2.0

operations team who investigate customers and should suspicious activity they will escalate the matter to MLRO via the Internal SAR procedure.

The Group conducts ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the casino's knowledge of the customer, their risk profile, including where necessary the source of funds.

- Customers who request to amend their personal information, will be required to provide suitable documentation to verify the change in information.
- A risk-based approach is applied in regards to obtaining up to date ID documents, when a customer is requested to provide new documents, any pending withdrawals will be held until satisfactory documents received.

12. Enhanced Ongoing Monitoring

Customers who are marked high risk by the business's customer risk scoring mechanism must firstly undergo enhanced due diligence but are then monitored on a monthly basis until such point they are no longer considered high risk by the model.

13. Internal Controls

Internal control procedures have been designed to comply with the regulations. Internal controls take the form of manual controls implemented on a daily basis by Group operations teams and computer/automated controls inherent within the gaming system software.

The gaming system has inbuilt internal control tools which based on the information inputted by the prospective customers can trigger red flags about suspicious activity to the operations team. Refer to some examples below:

- i. ***Prevention of multiple accounts held by same user:*** Inbuilt system checks confirm whether the email provided by the prospective customer is unique in the customer database preventing the possibility of a player having multiple accounts. If a player tries to open more than one account, for whatever reason, The Group reserves the right to block or close any or all of the player's accounts at its discretion.
- ii. ***Detection of any underage registrations:*** Underage registrations are automatically not allowed by the system.
- iii. ***No cash and no credit policy:*** Credit card deposits are accepted by the system only if the customer enters a valid credit card number with sufficient funds. A player can participate in any game only if the player has sufficient funds on his/her account for such participation. It is The Groups policy not to accept cash and not to give any credit whatsoever for participation in any game.
- iv. ***Withdrawal is only allowed if the name of person requesting the withdrawal is the same name of person holding the account:*** The Group's policy is that it shall only affect pay-out to an account, card, wallet, or similar instrument in the name of the player receiving pay-out.

Under no circumstances shall The Group affect a pay-out to a player in a name other than in the name of the player. Note, The Group rely on 3rd party payment providers verifying the name of account holder for bank transfer payouts.

Internal controls are not entirely computer dependent. The operations teams also has an important part in detecting and preventing money laundering. The below are a number of controls operated by the operations team:

- i. On-going monitoring and assessment of player's risk indicators and changes in players patterns.
- ii. On a daily basis a deposits report is reviewed by the payment and risk department and follow ups made on suspicious transactions deposits.
- iii. Monitoring of large deposits and withdrawals and/or deposits and immediate withdrawals or withdrawals with insufficient gameplay.
- iv. All withdrawals are checked and approved by the team
- v. The operations team confirm that the name of person requesting the withdrawal is the same name as person holding the bank account. Suspicious credit card deposits, transactions and accounts are followed up by a verification process including outbound calls.
- vi. Customer log activity is regularly analysed for indications of suspicious activity.

Additional verification on suspicious deposits, transactions or accounts will include, but not limited to:

- vii. Call Player to verify telephone number, take note of player's response/phone manner in call. This call is made by support staff in the same language of the player account.
- viii. Check if player exists on local country phone book, tax records, electoral register, additional public databases, with the same information.
- ix. Request additional ID, proof of address and copies and statements of bank or credit cards.

The management team have stats on the volumes such procedures are yielding and perform monthly quality checks on agent work done sampling at least 25 cases per agent.

14. Counter-Terrorist Financing

All customers are checked against the PEP & Sanctions database upon making their first deposit, if the customer is confirmed on any sanctions lists, their account is closed and an internal suspicious transaction report completed and escalated to the MLRO.

To comply with the United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. Upon notification of a sanctioned person playing on any of the sites across the group, any funds held on the gaming account with frozen and reported to the FIU immediately.

15. Politically Exposed Person

A Politically exposed person check is completed upon the customer making their first deposit (establishment of business relationship), if the customer is confirmed as a PEP the account will be

closed and if applicable deposits will be refunded.

The business checks if customers are PEPs on the outset of the business relationship when the customer first deposits using Comply Advantage (via Sum substance our KYC vendor) and uses constant ongoing monitoring for changes in PEP or sanctioned person databases (EU, UN, OFAC – levels 1- 4).

16. Known Criminals

As part of Comply Advantage checks, adverse media checks are completed including checks against public media for known convicted criminals, please see the Customer Acceptance Policy concerning the treatment of known criminals.

17. Suspicious Transaction Reporting (STR)

The Group is required to adhere to the stipulations of the National Ordinance for Identification of Services and to detect and report either intended or unusual transactions. Trenta Tech Group has implemented adequate procedures to cover:

- The recognition of unusual transactions.
- The documentation of unusual transactions.
- The reporting of unusual transactions.

The Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, state the following transactions or intended transactions are deemed unusual

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or the Department of Justice
- Transactions by or on behalf of a natural or legal person, a group or an entity, that is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55)
- Transactions in the amount of NAf. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 - A cashless transaction in the amount of NAf. 5,000 or more.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client
 - A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
 - Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
 - A cash out in the amount of NAf. 5,000 or more;

The MLRO will report an individual to the Curacao financial intelligence unit(s) if there is suspicion that the individual is laundering money, financing terrorist activities, or funding their gambling from the proceeds of crime.

If employees are in a position where they suspect that someone is laundering money or using the

proceeds of crime, then they are required to report their suspicion using a pre-defined form called an Internal STR and submit it to the MRLO. Please see Appendix A

Once this information has been received, the MRLO acknowledges and, as soon as practicable, reviews the information to determine if further profiling is appropriate.

In circumstances where the business receives an information request from law enforcement agents, the MLRO will decide whether to raise an External STR to the Financial Intelligence Unit.

18. High-Risk Jurisdictions

Geographical risk assessment is conducted on all countries that The Group accepts customers, the assessment will be completed using the below lists:

- FATF Jurisdictions under Increased Monitoring
- FATF/CFATF High Risk Jurisdictions subject to a Call for Action
- EU List identifying high risk 3rd countries with strategic deficiencies
- The US Department of State Money Laundering assessment (INCSR)
- Basel AML Index

The Group does not accept customers from any high-risk countries identified on the above lists, this is enforced by blocking players from playing from these countries. Enhanced due diligence will be requested on any customers who are resident from a high-risk country.

The Group may initiate enhanced due diligence when the person's nationality, country of birth, or transactions are from countries identified by the FATF and the CFATF.

19. Training

The Group will provide employees with an approved programme of training in relation to the topics and themes considered by the AML policy and procedures.

- A written record will be retained of all training received by employees.
- Training is required by all operational staff at onboarding
- All employees are required to complete refresher training annually.

20. Record Keeping

The Group shall maintain records containing the information and documentation necessary to complete the objective of the KYC measures referred to for at least five years after the business relationship is ended, or after 5 years from the date of the last occasional transaction. The business also keeps a record of real money transactional information according to the same policy.

21. Employee Vetting

We follow high ethical standards in the recruitment of all our staff. This includes taking prospective employees professional background into account, performing background checks, and verifying references provided from former employers, as per HR processes.

22. Policy Distribution

All employees receive a copy of the AML policy and other associated policies upon induction, and each year, once a review is completed and signed, the new AML documents are circulated to all staff, including subcontractors and Third-party suppliers when applicable by email, including a summary of any material changes.

23. Due Diligence for Third Parties

The company has processes in place, when applicable, to carry out due diligence upon establishing a business relationship in line with our regulatory requirements and to ensure that the company only works with reputable entities.

24. Policy URL

This policy cannot be accessed online through the company website.

25. Compliance and Consequences of Non-Compliance

The company is obligated to apply to all regulations covered under section 2 of the regulatory framework within this policy. Should Trent Tech Group violate these regulations, the company can be subject to disciplinary actions, legal implications, or business risks.

In situations of non-compliance, the following actions could be taken:

1. The company will be subject to regulatory fines.
2. Regulatory enforcement.
3. Respective action on particular regulations and processes.
4. License revoked.
5. Assess adequately the risk of money laundering or terrorist financing.

Contact Information

Any questions regarding this policy, please contact:

Name – Mark Taylor

E-mail Address – markt@diligenzagroup.com

Contact Number - +356 99911164

Appendix 1:

Internal Suspicious Money Laundering Report Specific to Employees to be submitted to the Money Laundering Reporting Officer

Instructions for completion of the form

It is your legal duty and a requirement of your employment with this practice that you report any knowledge or suspicion concerning money laundering to the firm's MLRO.

In accordance with our internal procedures, you need to complete the report form as quickly as is practical. Should any delay be likely you need to contact the MLRO immediately.

The form should be completed and sent via e-mail. Please do not take any copies.

Tipping off is a criminal offence. You should therefore avoid discussing your suspicions or concerns with anyone other than the MLRO in all but the most unusual circumstances.

Failure to comply with these requirements may result in action being taken against you in line with the Groups usual disciplinary procedures.

To: The Money Laundering Reporting Officer
Date of the report: [Insert date]
Prepared by: [Insert name and position]
Name & Player ID of individual(s) suspected: [Insert name of all individuals suspected]
Name & Player ID of client (if different): [Insert client name or confirm that no difference from the list above]
Reason for suspicion: [Give a detailed description of the reasons for your knowledge or suspicions. Please include supporting documentation if applicable]
Date suspicion first aroused: [insert date]
Names of all other colleagues who have been involved with this client's affairs: [Insert name of all individuals informed – each of whom should sign the declaration below]

Declaration

I am aware of the risks and penalties regarding "tipping off," or investigation of the above or related matters by the authorities.

Name:	Signed:	Dated:
--------------	----------------	---------------

--	--	--

Appendix 2:
Form to be completed by the Money Laundering Reporting Officer
upon receiving the above report from an Employee

Date received _____

Consideration of Disclosure:

Action Plan:

Outcome of Consideration of Disclosure:

Are there reasonable Grounds for suspicion?

Is consent required from the Financial Intelligence Unit (FIU) to any ongoing or imminent transactions which would otherwise be prohibited acts?
Y YES Y NO

If YES, please record authorisation and “way forward” details received from the Financial Intelligence Analysis Unit

If there are reasonable grounds to suspect Money Laundering, but you do not intend to report the matter to the FIU, please set out below your reasons for non-disclosure

Signed _____ Dated _____

THIS REPORT SHALL BE RETAINED FOR A MINIMUM OF FIVE (5) YEARS