



Curacao Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and Sanctions Compliance Policy

Code	AML-CUR-POL-01
Version	1.9
Date of version	May 28, 2025
Created by	Head of Risk & Compliance, MLRO
SME	Head of Risk & Compliance, MLRO
Approved by	Head of Risk & Compliance, MLRO
Confidentiality level	Medium

Document Version Control

Version	Update	Author	Date
0.1	Policy document creation	Erik Vogelgesang	13/06/2023
1.0	Approval of Policy	Niki Metzgar	02/08/2023
1.1	Addition of section on Reliance & Outsourcing	Erik Vogelgesang	04/08/2023
1.2	Amendment of grace period given for EDD completion	Flora Katsiana	22/08/2023
1.3	Document adjustment to reflect Curacao license requirement only	Magdalena Roszak-Kwiatek	22/12/2023
1.4	Update on Customer Acceptance/Rejection and Accounts Closures	Magdalena Roszak-Kwiatek	27/06/2024
1.5	Addition of section on Funds Management	Magdalena Roszak-Kwiatek	12/07/2024
1.6	CDD trigger update	Magdalena Roszak-Kwiatek	30/08/2024
1.7	Update in Customer Acceptance/Rejection Section, and change of final approver from Group Counsel to Group MLRO	Magdalena Roszak-Kwiatek	07/11/2024
1.71	Update on record keeping timeframes	Flora Katsiana	12/12/2024
1.8	Approval of record keeping timeframes updates	Magdalena Roszak-Kwiatek	12/12/2024
1.9	Overall review of the policy - update in accordance to the Curacao most current requirements	Magdalena Roszak-Kwiatek	28/05/2025

Table of Contents

1. Policy Statement.....	6
1.1 Purpose.....	6
1.2 Updates to the Document	6
1.3 Classification & Audience	6
1.4 Definitions.....	6
1.5 Outsourcing & Reliance	7
2. Policy Implementation.....	8
2.1 Overview.....	8
2.1.1 Money Laundering.....	8
2.1.2 Importance of ‘Knowledge’, ‘Suspicion of’ and ‘Reasonable grounds to suspect’	9
2.1.3 Terrorist Financing.....	9
2.2 Employee Obligations	11
2.2.1 Reporting Suspicious Activity.....	11
2.2.2 Corporate Responsibility	11
2.2.3 Anti-Bribery & Corruption	11
2.3 Money Laundering Reporting Officer (MLRO).....	12
2.3.1 Contact Information	12
2.4. Risk Assessment.....	13
2.4.1 Business ML & TF Risk Assessment (BRA).....	13
2.4.2 Risk-based Approach (RBA)	14
2.5. Customer Acceptance/Rejection Policy.....	15
2.6. Accounts Closures.....	16
2.7. Customer Risk Rating	17
2.8. Customer Due Diligence (CDD)	18
2.8.1 Identification.....	18
2.8.2 Verification	18
2.8.3 Corporate Due Diligence.....	18
2.8.4 Corporate Accounts	18
2.9. Watchlist Screening	20
2.9.1 Politically Exposed Person (PEP).....	20
2.9.2 Sanctions.....	20

2.9.3 Adverse Media	20
2.9.4 Timing of Checks	21
2.10. Enhanced Due Diligence (EDD)	22
2.10.1 Source of Wealth (SOW)	22
2.10.2 Source of Funds (SOF)	22
2.10.3 EDD Thresholds	22
2.10.4 Ongoing Monitoring	22
2.10.5 Incomplete EDD	23
2.11. Suspicious Activity	24
2.11.1 Suspicious Activity - Terrorist Financing	24
2.11.2 Suspicious Activity - Money Laundering	24
2.11.2.1 Suspicious Customer Behavior	24
2.11.2.2 Unusual Activity	24
2.11.2.3 Funding Instruments	24
2.11.2.4 Pattern of refund requests	25
2.11.2.5 High-Risk Jurisdictions	25
2.11.2.6 Unwillingness to complete a verification request	26
2.11.2.7 Linked Accounts Betting	26
2.11.2.8 Notification from an external source	26
2.11.2.9 Change in Country or Residence	26
2.11.2.10 Match Fixing	26
2.11.2.11 Problem Gambling and Money Laundering	26
2.12. Internal Suspicious Activity Reporting (ISAR)	27
2.13. External Suspicious Activity Reporting (SAR)	28
2.13.1 SAR Reporting Entities	28
2.13.2 Seeking a defense to a money laundering or terrorist financing offence (DAML)	28
2.13.3 Decision to Report	28
2.14. Closed Loop Policy	29
2.15. Record Keeping	30
2.16. Independent Review	31
2.17. Training	32
2.18. Funds Management Policy	33
3. Appendices	34
3.1 Applicable Legislation and Regulation	34

3.2 Employee Offences	34
4. Supporting Documents	35

1. Policy Statement

1.1 Purpose

This policy constitutes the core policy of Ragnarok Corporation N.W. , operating under the “Pinnacle” brand name, on Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and Sanctions Compliance, including an overview of various legal frameworks, risk management and mitigation strategies and Pinnacle’s responsibilities as employees to comply with relevant national, supranational, and sector-specific AML, CTF and Sanctions laws, regulations, and guidance.

Ragnarok Corporation N.V. will thereafter be referred to as “Pinnacle”.

1.2 Updates to the Document

The Head of Risk & Compliance/MLRO is responsible for implementing any updates to the document and reviewing it regularly, annually at a minimum or when material changes occur, to ensure the document remains relevant to changing business and regulatory requirements. Specifically, this document is updated in conjunction with updates to the ML & TF Risk Assessment (“BRA”). The Group MLRO approves the Policy.

1.3 Classification & Audience

This document is for internal use only, affecting all Pinnacle’s employees and subcontractors, and should not be taken off site or disclosed to third parties. There may be circumstances where this document will need to be shared with third parties, such as regulators, auditors, and financial institutions. Prior to sharing with third parties, employees should consult with the Head of Risk & Compliance/MLRO.

1.4 Definitions

For this document's purpose, the terms Suspicious Transaction Report (STR) and Suspicious Activity Report (SAR) are interchangeable.

Further, the following acronyms are used in this policy:

- AML - Anti-Money Laundering
- CTF - Counter-Terrorist Financing
- CDD - Customer Due Diligence
- EDD - Enhanced Due Diligence
- ISAR - Internal Suspicious Activity Report
- KYC - Know Your Customer
- ML - Money Laundering
- MLRO - Money Laundering Reporting Officer
- OFAC - Office of Foreign Assets Control (US)

- PEP - Politically Exposed Person
- SAR - Suspicious Activity Report
- SCP - Sanctions Compliance Programs
- TF - Terrorist Financing

1.5 Outsourcing & Reliance

Pinnacle does not outsource any of its AML & CTF functions. Reliance is merely placed on specific external tools and services, which are ultimately operated and controlled by Pinnacle employees.

2. Policy Implementation

2.1 Overview

2.1.1 Money Laundering

Money Laundering (ML) is the process by which criminals disguise the original ownership and control of the proceeds of crime to make such proceeds appear having derived from a legitimate source. ML also seeks to help the criminal avoid detection, confiscation, and conviction.

Money Laundering is not restricted to money but applies to any criminally derived property.

The following acts constitute Money Laundering:

- **Acquiring:** Acquiring, using, or possessing criminal property
- **Arrangement (Assisting):** Becoming concerned in an arrangement in which the offender knowingly suspects or facilitates the acquisition, retention, use or control of criminal property
- **Concealing:** Concealing, disguising, converting, transferring, or removing criminal property

Stages of Money Laundering

Money Laundering traditionally involves the following stages:

- **Placement** – Illegal funds are placed into the financial system either directly or indirectly by a money launderer.
- **Layering** – For money laundering to be successful, a money launderer needs to disguise the source of the criminal property. Layering separates the criminal property from their illegal origin by disguising or confusing the audit trail.
- **Integration** – Illegally derived funds are integrated into apparent 'legitimate' streams of income (e.g., gambling winnings).

A money launderer can use online gambling facilities at every stage of the process. Although remote gambling might be considered less vulnerable to the placement stage, since electronic transfers are required for placement, the layering stage is most likely the entry point for ML into Pinnacle.

'Lifestyle or Criminal Spend'

Money Laundering in gambling also includes criminal proceeds to fund gambling as a leisure activity. This is known as 'lifestyle spend' or 'criminal spend' and counts towards ML offences equally.

2.1.2 Importance of 'Knowledge', 'Suspicion of' and 'Reasonable grounds to suspect'

Pinnacle employees are required to report any **knowledge of, suspicion of or reasonable grounds to suspect** the existence of ML or TF. Failing to report knowledge or suspicion is an offence explained in further detail throughout the document.

It is important to remember that 'proceeds of crime' refers to the profit (benefit) made from ANY crime. Any person knowingly dealing with the proceeds of crime is conducting a money laundering offence.

What is 'Knowledge'?

Knowledge is actually knowing something to be true. Knowledge is not subjective but objective.

What is 'Suspicion'?

Suspicion goes beyond mere speculation and is based on some foundation. A transaction that is unusual is not necessarily suspicious. An unusual transaction should be queried and if no reasonable explanation is provided, suspicion may be formed. Suspicion is not objective but subjective.

What are 'Reasonable Grounds to Suspect'?

We have an obligation to make a disclosure even in cases where there are 'reasonable grounds to suspect'. The obligation to report exists also when based on objective facts that a suspicion should have been formed.

2.1.3 Terrorist Financing

What is 'Terrorist Financing'?

Terrorist Financing (TF) occurs where an individual or group provide or facilitate the provision of funds, premises, people, or resources for terrorist activity. Unlike ML, where funds always originate from illegitimate sources, the funds in TF can originate from legitimate OR illegitimate sources.

All dealings with funds or property, which are likely to be used for the purpose of terrorism, even if the funds are 'clean in origin', constitute a terrorist financing offence.

Terrorist Financing Offences

Terrorist Financing offences are considered below:

- **Fundraising** – Fundraising or contributing to an organization or person if there is knowledge or suspicion that the funds may be used for terrorist purposes.
- **Use or possession** – Using or possessing money or property for terrorist activity.

- **Arrangements** – Becoming concerned in an arrangement that makes money or property available for terrorist purposes.
- **Money Laundering** – Laundering terrorist property, e.g., 'concealing, removing, or transferring terrorist property to a third party.

2.2 Employee Obligations

2.2.1 Reporting Suspicious Activity

If a Pinnacle employee knows or suspects that any customer activity is linked to ML or TF, they must report this immediately.

The Pinnacle employee must send an internal Suspicious Activity Report (ISAR) via the standardized form and email (mlro@pinnacle.com) to the MLRO directly. Alternatively, the employee shall escalate potential suspicious behavior by creating standardized JIRA sub-ticket, notifying the MLRO/Deputy MLRO via the relevant 'aml-mlro' Slack channel.

The obligation to report remains with the individual employee, irrespective of whether they consulted with their colleagues.

Please see the relevant sections on ISARs and SARs further down below. Please refer to ISAR and SAR Procedure for further reference. Please see Annex for applicable employee offences.

2.2.2 Corporate Responsibility

Pinnacle and its Board of Directors have a corporate responsibility to prevent ML and TF. The following are their main obligations:

- Fulfill regulatory requirements with regards to the prevention of ML and TF
- Put in place and update adequate policies, procedures, and controls to mitigate the risk of ML and TF
- Facilitate staff awareness regarding the risks of ML and TF
- Implement an employee training program for the prevention of ML and TF
- Review and approve the organization's AML, CTF and Sanctions Compliance program
- Ensure that adequate resources are made available to the Compliance function
- Ensure that senior management gives appropriate autonomy to the Compliance function
- Meet periodically with the Compliance function to ensure Pinnacle is fulfilling legal and regulatory duties

2.2.3 Anti-Bribery & Corruption

It is illegal to offer, promise, give, request, agree, receive, or accept bribes.

Employees must refer to Pinnacle's Anti-Bribery and Corruption (ABC) Policy, which is made available to all employees via the Pinnacle Wiki and training portal (X-Center).

2.3 Money Laundering Reporting Officer (MLRO)

Pinnacle is required to maintain an MLRO function for Curacao jurisdiction.

Role of the MLRO

The MLRO and their Deputy are responsible for the following:

- Receiving internal Suspicious Activity Reports (ISARs)
- Considering ISARs received and evaluating whether there is ML or TF involved
- Reporting any suspicious activity via Suspicious Activity Reports (SARs) to the appropriate authorities
- Where necessary, obtain consent to proceed with a reported transaction
- Put in place and operate AML/CTF and Sanctions Compliance policies, procedures, and controls
- Carry out periodic effectiveness reviews of the existing AML & CTF and Sanctions Compliance program
- Carry out business-wide ML & TF and Sanctions risk assessments
- Record keeping
- Employee training in preventing ML, TF, and sanctions evasion
- Ensures that Pinnacle fulfills its obligations under relevant national and supranational legislation and regulation

Deputy MLRO

When the MLRO is temporarily not able to exercise his/her duties Deputy MLRO takes over temporarily, until the MLRO can fulfill his/her roles again.

2.3.1 Contact Information

For any questions regarding this policy, please contact:

- Head of Risk & Compliance/MLRO – Erik Vogelgesang
email address: erik.vogelgesang@pinnacle.com
- Financial Crime Risk Manager & Deputy MLRO – Magdalena Roszak-Kwiatek
email address: magdalena.roszak-kwiatek@pinnacle.com

2.4. Risk Assessment

2.4.1 Business ML & TF Risk Assessment (BRA)

The MLRO maintains jurisdiction-specific BRAs for the business. These documents are reviewed periodically and when material changes occur and signed off by the Pinnacle Board.

The below outline is designed to provide a summary for staff to be aware of the main areas of risk. Additional detailed information is contained in the relevant BRA document itself.

Customer Risk

The risk a customer presents can depend on many factors e.g., third party funding, links to fraudulent accounts, peer-to-peer activity, betting with linked accounts, Politically Exposed Person (PEP) involvement, or links to high-risk jurisdictions.

Transactional Risk

Risks may be inherent in the transactional aspects of the business that can be used to facilitate ML and TF. As examples, customers who deposit large sums of money or engage in specific patterns of transactions designed to avoid detection are considered as potential risks.

Product Risk

The level of product risk depends on whether product or service characteristics are conducive to ML or TF. In casino products, such as Poker and Roulette, where players can lose money to another player, the product risk is deemed higher due to the collusion aspect.

Delivery Channel Risk

Delivery channel risk relates to how a product or service is marketed and delivered. Non-face-to-face onboarding of customers or third-party management of parts of the remote gaming process by gaming providers can attract financial crime.

Geographic Risk

Geographic risk increases in countries with higher crime rates, unstable governments, high corruption rates, weak Anti-Money Laundering (AML) / Counter-Terrorist Financing (CTF) regimes or being subject to financial sanctions.

Governance Risk

Pinnacle is committed to creating a well-resourced, robust AML & CTF compliance function. The MLRO provides regular reporting to senior management and Pinnacle Board on all matters relating to AML & CTF compliance including performance against AML, CTF and Sanctions Compliance requirements.

2.4.2 Risk-based Approach (RBA)

By adopting a Risk-based Approach, Pinnacle determines the extent of the application of CDD and EDD requirements on a risk-sensitive basis. To utilize limited resources most effectively, efforts are geared towards risk mitigation areas where most needed and having the most impact. Hence, resources are directed proportionately in accordance with the ML/TF/Sanctions risk posed. The RBA will determine:

- Extent of identification and verification thereof sought by Pinnacle
- Additional information to be requested how information is verified
- Monitoring efforts throughout the relationship

2.5. Customer Acceptance/Rejection Policy

Based on the requirements of various statutory obligations, Pinnacle has taken a position on who they can and cannot accept as a customer.

An applicant cannot engage in gaming with Pinnacle unless that person is registered as a player and holds an account with our company.

To successfully register an account, potential customers need to provide Pinnacle with their personal details.

At minimum:

- First and last name,
- Residence address
- Email address
- Date of birth
- Country of registration
- Contact phone number

Each account is secured with the password created by the user, security question and answer known only to the owner of the account.

All customers with intentions to avail themselves of remote gaming services shall be accepted, unless they meet criteria listed below.

Pinnacle does not accept individuals who:

- Are less than eighteen (18) years old,
- Would not have intention to avail themselves of remote gaming services,
- Politically Exposed Persons (PEPs) who may represent risk not acceptable by company,
- Whose name is included in any Financial Sanction Lists compiled by the United Nations (UN), the EU and other relevant authorities,
- With relevant Adverse Media found against their name who may represent risk not acceptable by company,
- Have been identified or suspected to have committed acts of fraud or bonus abuse with other operators,
- Are identified to have been involved, suspected of, known to be associates of individuals involved in criminal activities or have a bad reputation.

Please see Section 2.6, 2.8 and 2.10 of this document as well as Watchlist Screening Procedure for further reference.

2.6. Accounts Closures

All accounts can be closed either by customers themselves or by Pinnacle.

There are three (3) types of accounts closures available for Pinnacle's employees:

- Self-exclusion – for definite or indefinite period of time
- Deactivation – for definite or indefinite period of time
- Permanent closure

With AML/CTF related teams using only permanent closure.

Aside for closure, AML related teams have the ability to also suspend or freeze the account. Whereby suspension Pinnacle understands account blockade where the customer has no ability to make any transactions or place a bet and no ability to log into the account.

By account freeze, Pinnacle understands account blockade where customer cannot make any transaction or place a bet but can log into the account.

Account can be closed by AML, FIP or CSD Team due to:

- Failure to comply with regulatory requirement (KYC/CDD/EDD) – within specified by relevant procedure timeframe, failure to obtain or insufficient documents were provided for due diligence purpose, and account risk has been assessed as not acceptable by Pinnacle
- Suspicion of money laundering or terrorist financing
- Fraud is detected

Account can be suspended by AML Team due to:

- Failure to comply with regulatory requirements (SOF/SOW) – within specified by relevant procedure timeframe, failure to obtain or insufficient documents were provided for due diligence purpose, yet no reasonable grounds to suspect money laundering or terrorist financing has been found
- Strong potential PEP or Adverse Media, or true, match – account awaits Senior Management decision
- AML or Fraud investigation

Account freeze is applied due to:

- Strong potential PEP or Adverse Media match – account awaits Senior Management decision
- Failure to provide, within specified by relevant procedure timeframe, documents related to CDD/EDD process
- AML investigation

Please see ID&V, EDD, iSAR and SAR Procedures for further reference.

2.7. Customer Risk Rating

In addition to existing transactional threshold alerts, Pinnacle operates an automated AML Risk Scoring Model. The model scores all customers as low / medium / high initially upon first deposit and on a 24-hr rolling period based on several factors further outlined below:

- Payment Method Risk type (e.g., higher weighting for prepaid cards & eWallets)
- Geographic region customer is registered from (higher weighting for high-risk jurisdictions)
- Transactional activity (higher weighting for activity considered unusual for Pinnacle customers, e.g., no/minimal play and requesting withdrawal)
- Product Risk (product used by the customer, i.e., Sportsbook and/or Casino)

High Risk accounts will immediately trigger an EDD (incl. SOF & SOW) review, and enhanced ongoing monitoring will be applied.

Furthermore, a Manual Risk Assessment must be conducted when receiving transactional threshold alerts or escalations from operational departments. The Manual Risk Assessment takes into consideration all the aforementioned factors along with open-source findings, as well as results from Watchlist Screening conducted:

- Watchlist Screening
 - PEP (auto-high risk)
 - Sanctions (auto-high risk/off-boarded)
 - Adverse Media status (risk depends on level of Adverse Media)

Where risk is deemed as high, EDD (incl. SOF & SOW) review conducted.

Please see the AML Customer Risk Rating Procedure for reference.

2.8. Customer Due Diligence (CDD)

2.8.1 Identification

Identification is the process of obtaining personal details, entity information and other relevant information about a player or business partner e.g., name, surname, age, nationality, date of birth in the case of a player or the name, company registration number, address, and jurisdiction of incorporation of a company.

Please see the Customer Identification & Verification Procedure for further reference.

2.8.2 Verification

Verification is the process of verifying the information obtained based on documents, data or information obtained from a reliable and independent source e.g., in the case of a customer, Pinnacle checks name, surname, address and date of birth against a Government issued document such as passport or ID card or using third party document verification software (i.e. SumSub).

Curacao customers are verified upon the financial threshold trigger of NAF 4,000 lifetime accumulation of deposits and withdrawals, where withdrawals are not treated as negative numbers.

Please see Customer Identification & Verification Procedure for further reference.

2.8.3 Corporate Due Diligence

Before accepting a corporate customer or entering a business relationship with any partner or supplier where Pinnacle is subcontracting part of the licensed function, Pinnacle will perform its own due diligence.

See Corporate Due Diligence Procedure for details of the identification & verification procedures for corporate customers and other business relationships.

Affiliates

CDD for affiliates must be conducted prior to opening an account.

- Where the affiliate is an individual, Pinnacle needs to verify the identity and address by obtaining documents
- Where the affiliate is a corporate entity refer to the section above

For affiliates, both individual and corporate, Pinnacle obtains their VAT or tax registration number.

2.8.4 Corporate Accounts

Corporate Accounts are individuals betting on behalf of other individuals as proxy or another third-party. These are usually operated by one individual funded by many other individuals. This makes it difficult to establish and trace the Source of Funds and Source of Wealth of all the individuals involved within the corporate account.

Pinnacle does not allow any form of new corporate accounts to operate on any of Pinnacle's websites. Existing corporate accounts on pinnacle.com are revisited in relation to their eligibility regularly and will get wound down depending on Pinnacle's assessment and at Pinnacle's discretion.

2.9. Watchlist Screening

2.9.1 Politically Exposed Person (PEP)

Politically Exposed Persons (PEPs) risk are risks associated with providing services to persons with a high political profile or who hold a public office. The definition of a PEP also extends to their immediate family and close associates. The PEP's office and position can leave them vulnerable to bribery and corruption.

To identify if a customer has PEP or PEP by association status, Pinnacle will run checks upon various trigger points in the customer journey on the customer using a professional Watchlist screening service provided by SumSub/ComplyAdvantage.

Pinnacle is not prohibited from doing business with PEPs or PEPs by association, however when a PEP is identified and confirmed, Pinnacle classifies the customer as high risk and applies EDD (incl. SOF & SOW) and Enhanced Monitoring.

Please refer to the Watchlist Screening Procedure for further reference.

2.9.2 Sanctions

Individuals and entities may be sanctioned based on foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction (i.e., 'proliferation financing'), and other threats to national security.

To identify if a customer is included on a Sanctions list, Pinnacle runs checks on the customer using a professional watchlist screening service provided by SumSub/ComplyAdvantage.

Where Pinnacle does determine that previous sanctions were applied to an individual but are not applied anymore (i.e., lapsed sanctions), this does not prohibit the individual from maintaining a business relationship with Pinnacle.

Business relationships with sanctioned individuals are prohibited and upon identification, the customer account will be closed, funds frozen and reported to the relevant authorities. Frozen funds and other blocked assets are not to be further handled until reported on and having received feedback from the relevant authorities.

Please see Watchlist Screening Procedure for further reference.

2.9.3 Adverse Media

Adverse media, or negative news, are unfavorable news or information considered to include allegations published by news sources on convictions for, or alleged involvement in, ML, TF, corruption, sanctions exposure, or other unlawful activity. For Adverse Media to be considered by Pinnacle, a financial crime nexus must exist. To establish whether a customer has relevant Adverse Media against their name, Pinnacle runs checks on the customer using a professional watchlist screening service provided by SumSub/ComplyAdvantage.

Please see the Watchlist Screening Procedure for further reference.

2.9.4 Timing of Checks

To determine the PEP, Sanctions or Adverse Media status of a customer, Pinnacle runs checks on the customer using a commercial database at specific intervals throughout the customer journey:

Initial Checks

- On 1st deposit

Periodic Checks

- On an ongoing basis via the SumSub/ComplyAdvantage Ongoing Monitoring Platform
 - Upon ID verification
 - Upon changes identified regarding name during verification processes
 - Upon changes to the relevant Watchlist(s)/data

2.10. Enhanced Due Diligence (EDD)

2.10.1 Source of Wealth (SOW)

Source of Wealth is the term used to describe how a customer or business partner generated their wealth or net worth (i.e., total body of wealth / assets).

In instances which present a higher risk for ML & TF (e.g., a PEP or customer from a high-risk jurisdiction), the source of wealth must be established. Pinnacle does not accept generic descriptions of the source, such as “savings” or “inheritance”, without undertaking further checks to establish the true information behind the generic description.

If the expected source of wealth does not correspond with the client profile, further checks regarding the source of wealth must be obtained, incl. supporting documentation were deemed appropriate.

2.10.2 Source of Funds (SOF)

Source of Funds refers to the origin and means used of the funds for a transaction. This information should include where (i.e., which institution) the actual funds are being remitted from e.g., bank account name, number, address, and sort code.

In instances where risks for ML and TF are higher, the source of funds must be established.

Please see EDD Procedure for further reference.

2.10.3 EDD Thresholds

For all accounts, Pinnacle operates a suite of risk-based financial threshold alerts to trigger an EDD review of a customer, including SOF & SOW checks.

Please see all current alerts referenced in the EDD Procedure.

Accounts will be given time to comply with the EDD request, where no restrictions on deposits/withdrawals/wagering will be applied for up to 14 days.

EDD checks are completed by the AML Team.

The procedure for conducting an EDD check is described further in the EDD Procedure.

2.10.4 Ongoing Monitoring

Pinnacle monitors accounts for different kinds of suspicious activity e.g., transactions with no apparent economic purpose.

Monitoring steps Pinnacle performs include:

- Ongoing monitoring of unusual transaction patterns and trends
- Checking ID and Proof of Address (POA) documents and explanations received

- Ensuring that CDD/EDD is ongoing, and identity records are updated if customer circumstances or personal details change (e.g., address change)
- AML Customer Risk Rating Model updating a customer's AML Risk Score every 24 hrs and Manual Risk Scoring on an ad hoc basis, as well as, where customers move between risk levels
- EDD checks are refreshed at regular intervals as per above description on triggers for New and Existing customers

2.10.5 Incomplete EDD

If a customer fails to send through their documents within 14 days, the account is suspended/fully restricted. Customers who partially provide documents can continue depositing/withdrawing/gambling up to 30 days after the EDD request.

Please see EDD Procedure for further reference.

2.11. Suspicious Activity

2.11.1 Suspicious Activity - Terrorist Financing

The following are a non-exhaustive list of red flags relevant to Pinnacle, which may indicate terrorist financing activity:

- Moving funds to and from high-risk countries and geographic locations with links to terrorism
- Gaming account usage with IP address links to high-risk jurisdictions with links to terrorism
- Unusual or suspicious religious quotes, or single words/phrases relating to known terrorist ideology
- Known numerical associations to terrorism in financial transactions and customer details
- Use of multiple foreign bank accounts to conduct transactions

Please see ISAR Procedure for further examples of terrorist financing red flags.

2.11.2 Suspicious Activity - Money Laundering

The examples below are associated with all customers and may indicate money-laundering activity

2.11.2.1 Suspicious Customer Behavior

The following are a non-exhaustive list of red flags relevant to Pinnacle, which may indicate money-laundering activity:

- Depositing amounts just below a particular threshold (e.g., set verification threshold)
- High frequency and value of bets in short time periods
- Account holds large balances which are not in line with betting behavior
- Minimal/no play post funds deposited and followed by request for withdrawal of funds
- Submitting fraudulent / false documents
- Unexplained or unclear source of funds or wealth
- Using higher risk forms of payment to fund a lower risk form of payment (i.e., using a crypto asset to fund a bank account used to deposit with Pinnacle)

Please see ISAR Procedure for further examples of money laundering red flags.

2.11.2.2 Unusual Activity

A transaction that appears to be unusual is not necessarily suspicious. Therefore, it is important to establish whether a customer's change of behavior remains merely unusual, amounts to suspicious activities OR the development of problematic gambling. The latter will need to be dealt with according to Pinnacle's Responsible Gambling Policy.

2.11.2.3 Funding Instruments

The following is a non-exhaustive list that constitutes examples of suspicious behavior in relation to usage of payment methods:

- Registering an unusually substantial number of payment instruments with their account
- Velocity of changing amount and usage of various payment methods
- Using a payment method that does not belong to the gaming account holder
- The place of issue of the payment method is different from the place of residence of the player
- The payment source, e.g., credit card or bank account originates from a high-risk jurisdiction
- High usage and velocity of changing prepaid cards
- Use of Crypto assets prior to funding the gambling account with another payment method
- Refused deposits on payment instrument

Please see ISAR Procedure for further examples.

2.11.2.4 Pattern of refund requests

Unusual refund or chargeback requests can indicate fraudulent activity. If there is a pattern of linked requests, this may indicate one of the following:

- Widespread financial crime e.g., fraud ring of linked accounts
- The collusion of a 'victim' with a 'fraudster'
- A 'problem gambler' attempting to fraudulently claim back spent funds

2.11.2.5 High-Risk Jurisdictions

Relationships regarding High-Risk Jurisdictions must be considered during a customer's risk assessment. Customers that are associated with higher-risk countries, because of their citizenship, country of business or country of residence may present a higher ML and/or TF risk. Pinnacle considers the following authoritative sources when assessing the country risk level regarding ML & TF:

- Financial Action Task Force (FATF)
 - Jurisdictions under Increased Monitoring (["Grey List"](#))
 - High-risk and other monitored jurisdictions (["Black List"](#))
- EU High-Risk Third Countries [List](#)
- www.knowyourcountry.com - [Ratings Table](#)
- Basel AML Index - [Public Ranking Table](#)

The following is a non-exhaustive list that constitutes examples of suspicious behavior in relation to high-risk jurisdictions:

- Withdrawals to bank accounts in high-risk jurisdictions, without reasonable explanation inconsistent with the customer's previous activity
- Deposits from high-risk jurisdictions and/or high-risk payment methods
- Funding currency does not match the currency in use in the jurisdiction where the player is located (e.g., Brazil-based player depositing in EUR)

Please see Customer Risk Rating Procedure for further reference to assessing and action on customers based on jurisdictional risk factors.

2.11.2.6 Unwillingness to complete a verification request

A customer is reluctant to comply with requests to verify their identity or respond to an EDD (incl. SOF & SOW) request. A refusal to provide a document is not a red flag on its own but may be so in combination with other risk indicators.

2.11.2.7 Linked Accounts Betting

When a customer uses certain casino products, such as Poker or Roulette, customers might be colluding with other customers (e.g., through deliberate losses).

A fraudster or group of fraudsters may use a series of stolen identities to fund several accounts and then bet and lose to another so that funds can be withdrawn as legitimate winnings.

2.11.2.8 Notification from an external source

Notification of unusual or suspicious activity can also come from external sources such as law enforcement agencies (LEAs), the police, regulators, payment processors or financial institutions. If any external requests for information (RFIs) are received, these must be directly escalated to the AML Team (incl. the MLRO & Deputy MLRO).

2.11.2.9 Change in Country or Residence

Pinnacle may detect that a customer is playing outside of their country of registration, which could indicate a red flag in terms of jurisdictional risk. Even if the customer may have legitimate reasons for having changed their location, Pinnacle must ensure they are playing on the correct product for that jurisdiction.

Please see Customer Identification and Verification Procedure for further reference.

2.11.2.10 Match Fixing

Pinnacle's customers can place wagers on fixed betting events or may be used by individuals involved in match fixing to spend proceeds of crime. This must be considered when reviewing account activity, particularly if it appears to have been created for wagering on known, fixed events.

2.11.2.11 Problem Gambling and Money Laundering

For a small percentage of customers, gambling can be difficult to control. Pinnacle provides customers with tools to help manage their play and actively monitors and interacts with customers considered at risk. Despite these controls, it is important to be aware that, for some individuals, problem gambling can act as a motivator to commit crime to fund their gambling. Pinnacle considers signs of potential financial distress when reviewing customer accounts. Where a customer cannot provide clear evidence of how they have afforded their gambling, or how they are funding their lifestyle, this may be an indicator of use of proceeds of crime.

Please see the EDD Procedure for further reference.

2.12. Internal Suspicious Activity Reporting (ISAR)

All knowledge or suspicion of ML/TF must be first reported internally to the MLRO who will then evaluate the report submitted and based on the report will decide whether to submit a report to the appropriate authority.

ISAR reports are reviewed as soon as possible once received by the MLRO.

External SARs are submitted to the relevant authorities once the MLRO has investigated the ISAR to an appropriate level but no later than 5 working days.

Please refer to the Internal Suspicious Activity Reporting (ISAR) Procedure for a full outline of the process.

2.13. External Suspicious Activity Reporting (SAR)

Upon receipt of an ISAR, the MLRO will decide whether to report the case to the relevant reporting authority. If Pinnacle anticipates an activity such as processing a withdrawal may result in committing a principal ML or TF offence, Pinnacle may request a defense from the relevant authority about a particular activity.

2.13.1 SAR Reporting Entities

Financial Intelligence Units (FIUs) per License

- Curacao FIU

The reporting entity will provide Pinnacle with a reference number for any SARs submitted.

2.13.2 Seeking a defense to a money laundering or terrorist financing offence (DAML)

Country / Reporting Authority	Reporting Regime
Curacao (FIU Curacao)	No DAML Regime. Requirement to promptly report an unusual transaction made or intended to be made to FIU.

2.13.3 Decision to Report

The MLRO/Deputy MLRO will review all ISARs and decide whether to make an external report. The MLRO will record a rationale for their decision in all instances.

A disclosure must be made where there are grounds for suspicion or knowledge that a person is involved in ML or TF.

There is no obligation to report where NONE of the following is known or suspected:

- The identity of the person engaged in money laundering or terrorist financing
- The whereabouts of any of the laundered property
- That any of the information that is available would assist in identifying that person, or the whereabouts of the laundered property

Please see further reference to the SAR process in the Suspicious Activity Reporting (SAR) Procedure.

2.14. Closed Loop Policy

To mitigate Financial Crime risk, Pinnacle operates a closed loop policy in relation to withdrawals of customer funds. Wherever possible, Pinnacle will process withdrawals and refund payments to the original method of deposit.

In exceptional instances where it is not possible to refund to the same method of deposit, extra measures will be taken to verify the player and the method to which Pinnacle will be sending the payment.

Exceptions:

- Amount(s) deposited from one payment method have already been covered via withdrawals to that payment method, and the sum being withdrawn is purely from winnings of wagers
- Original form of payment method where deposit(s) derived from is no longer available/expired

When an exception is being made, an additional layer of due diligence is required on the relevant customer account, such as:

- Processing the withdrawal to a lower risk payment method, such as, a bank transfer to an account the individual has proven is in their name
- Ensuring the relevant gaming account is not currently under investigation by the AML, RG, or Fraud Teams

2.15. Record Keeping

To comply with relevant national Money Laundering laws and regulations, Pinnacle must keep the following records for a minimum of 10 years after the end of the customer (business) relationship:

- Customer transaction history (incl. Deposit/Withdrawal figures, bets made, and the winnings paid out)
- Evidence Pinnacle collects to identify and verify our customers (incl. supporting documentation)
- The remote games of chance played;
- The number of times each game has been played;
- The players who participated in each game;
- The transactions of all players, including the bets made and the winnings paid out

Where a SAR is submitted, the 10-year period will start on the date the SAR is submitted.

Pinnacle must also keep the following records:

- Details of how compliance has been monitored by the MLRO/Deputy MLRO
- Delegation of AML/CTF tasks by the MLRO/Deputy MLRO
- MLRO reports to senior management
- Information not acted upon by the MLRO, with reasoning why no further action was taken
- Employee training records
- Internal and external Suspicious Activity Reports (ISARs/SARs)
- Reasons for not making an external SAR following an ISAR
- Contact between the MLRO and law enforcement or the regional investigation unit
- Records connected to appropriate consent/defense for Money Laundering (DAML)

2.16. Independent Review

Pinnacle must conduct an independent review of their AML & CTF program to assess its effectiveness. The primary purpose of the independent review is to determine the adequacy of Pinnacle's AML & CTF program, including whether the business is operating in compliance with the requirements of various national laws and regulations and Pinnacle's own policies and procedures.

The review must contain the following elements:

- Policies and procedures (incl. BRAs)
- Internal systems and controls
- Recordkeeping and reporting requirements
- Training
- Making recommendations regarding policies, procedures, systems, and controls
- Monitor compliance with recommendations

The review will be risk-based and must test Pinnacle's risk assessment for reasonableness and risk mitigation strategies in place. The review must also focus on testing the internal controls and transactional systems and procedures on a sample basis.

An independent review must be performed by a combination of second line (2nd LOD) and third line (3rd LOD) of defense resources, including Internal Audit or an appropriate external third party on a frequency determined by the business's risk appetite and in conjunction with the Pinnacle Board.

The MLRO and Group Counsel will review any reports produced and any deficiencies and weaknesses identified must be tracked for a timely resolution.

Any documentation requests will be made available to relevant authorities who can examine them.

2.17. Training

AML & CTF training at a minimum must be provided to employees who are responsible for the following:

- Handling or monitoring of transactions
- MLRO / CO incl. their Deputy
- Player onboarding and CDD/EDD
- Regulatory reporting
- Finance department handling customer and corporate funds
- Addressing Player queries or concerns (e.g., Customer Service)
- Technology functions related to AML activities
- Ultimate oversight of the AML & CTF program (Senior Management and Board of Directors)

Nature of training

Training must vary according to the role the member of staff occupies and will include practical examples on ML & TF typologies. Training will consist of internal and external training.

Frequency of training

Training must be provided at regular intervals based on the following trigger events:

- New employees
- Annually at a minimum
- At any other interval deemed necessary by management or the MLRO/Deputy MLRO

Records of training

Records of all AML/CTF training provided to all staff will be kept. These records will include:

- Date on which the train was delivered
- Nature of the training
- Names of members of staff attending the training
- Results of any assessment

2.18. Funds Management Policy

To remain in compliance with various regulatory regimes Pinnacle is subject to, this policy needs to be observed when handling and managing customer funds. Most importantly, payments must only be accepted and made from accounts held with licensed financial institutions (FIs) or through licensed payment service providers (PSPs).

Furthermore, the following conditions need to be adhered to:

- Pinnacle must guarantee that all the funds deposited by the customer or owned by Pinnacle must be credited to the customer's corresponding gaming account.
- Pinnacle must only remit withdrawals to the same account from which the funds originated, or if this is not possible, Pinnacle must verify that the alternative destination is secure and belongs to the same customer – please see section on Closed Loop Policy.
- Pinnacle prohibits cash deposits/withdrawals.
- Pinnacle guarantees that the back-end System must also be capable of generating a dated report pertaining to jackpot funds; inclusive of a timestamp which presents the information described under (i) to (iv) below (as a minimum, this report shall be generated as at end of day on the last day of each month);
 - i. Identifying aggregate jackpot funds (by currency);
 - ii. Distinguishing between jackpot provider;
 - iii. Distinguishing between local and pooled jackpots;
 - iv. Distinguishing between jackpots falling under the Maltese license and jackpots falling under any foreign licenses.

Both system reports mentioned above must not constitute an Excel, Word, csv, or pdf file. The system must produce the report using a front-end application, which demonstrates the information through the application itself.

3. Appendices

3.1 Applicable Legislation and Regulation

Curacao

- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- National Ordinance on Identification When Rendering Services (NOIS)
- National Decree on Supervisor Identification When Rendering Services in the Gaming Sector (no. 19/0282)
- National Decree on Supervisor of Unusual Transactions in the Gaming Sector (no. 19/0283)

3.2 Employee Offences

The following table summarizes the key offences linked to ML / TF, which any employee of Pinnacle can commit, and the maximum penalties associated with such action in the various licensed jurisdictions:

Curacao			
Offence	Failure to disclose	Tipping off	Prejudice an investigation
Reason	The employee knows, suspects or should have known or suspected that ML or TF is involved and fails to report.	Prohibited disclosures (tipping off).	Disclosing the fact that an STR was created, or disclosing the contents of such a report, with the intent to harm a criminal investigation.
Criminal Sanction	• Fine not exceeding NAF 10,000 • Or imprisonment for a period not exceeding 1 year	• Fine not exceeding NAF 10,000 • Or imprisonment for a period not exceeding 1 year	• Fine not exceeding NAF 10,000 • Or imprisonment for a period not exceeding 1 year

4. Supporting Documents

Document Name	Document Type
AML & CTF Risk Assessment	Business Risk Assessment
AML Customer Risk Rating Procedure	Procedure
Anti-Bribery and Corruption (ABC) Policy	Policy
Corporate Due Diligence Procedure	Procedure
Customer Identification & Verification Procedure	Procedure
Enhanced Due Diligence Procedure	Procedure
Internal Suspicious Activity Procedure	Procedure
Suspicious Activity Procedure	Procedure
Watchlist Screening Procedure	Procedure