

**Policy for Prevention and Combatting of Money Laundering, Terrorist Financing and Counter-Proliferation Financing**

**Green Point Technology NV**

**July 2025**

| Draft Version | Change Details | Amended By         | Board of Directors Approval Date |
|---------------|----------------|--------------------|----------------------------------|
| 1             | Initial Draft  | Compliance Officer | 22/07/2025                       |
|               |                |                    |                                  |
|               |                |                    |                                  |
|               |                |                    |                                  |

### **Control Statement**

This Manual is the property of Green Point Technology NV, and it is a highly confidential and controlled document. It is not to be reproduced, distributed or used without written permission from the Board of Directors.

### **Recipients:**

- Board of Directors
- Compliance Officer
- Internal Auditor
- Compliance/AML Team
- Customer Support Team
- Accounting Team

### **Relevant Legislation and references:**

- The National Ordinance on Identification of Clients when Rendering Services NOIS (N.G. 2017, no 92)
- The National Ordinance on the Reporting of Unusual Transactions NORUT (N.G. 2017, no.99)
- The Sanctions National Ordinance (N.G. 2014, no.55).
- The Kingdom Sanctions Act (N.G. 2016, no.54).
- National Ordinance for Games of Chance (LOK)
- National Ordinance Penalization of Money Laundering (NOPML)
- Regulation Indicators Unusual Transactions (N.G. 2015, no. 73);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Decree for General Measures, 10 July 2015 (N.G. 2015, no. 29);
- National Decree for General Measures, 10 July 2015 (N.G. 2015, no. 28);
- National Decree for General Measures, 10 July 2015 (N.G. 2015, no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- Regulations for the combating of ML/TF and Proliferation of weapons of mass destruction of the Curacao Gaming Control Board of January 2025;
- The Financial Actions Task Force ("FATF").
- The Basel Committee on Banking Supervision.
- The Wolfsberg Group.
- The Egmont Group.
- Regulators, such as guidance and the reasoning set out in regulatory fines.
- Financial Intelligence Units ("FIUs") and law enforcement agencies, such as threat reports, alerts and typologies.
- Information obtained as part of the Customer Due Diligence process.
- Industry bodies, such as typologies and emerging risks.
- Civil society, such as corruption indices, transparency indices and country reports i.e. Basel AML Index.
- International standard-setting bodies such as mutual evaluation reports or legally non-binding blacklists.
- Credible and reliable open sources.
- The Company's own knowledge and professional expertise.

## Directory

|                                    |                                                                                     |
|------------------------------------|-------------------------------------------------------------------------------------|
| Company Name                       | Green Point Technology NV                                                           |
| DBA                                | Citobet                                                                             |
| Date of Incorporation and domicile | 23/03/2023 / Curacao                                                                |
| Registration Number                | 163399                                                                              |
| Board of Directors                 | Morganite Corporate Services BV                                                     |
| Compliance Officer                 | Christos Polyviou                                                                   |
| Internal Auditor                   | N/A                                                                                 |
| Registered Office                  | Abraham de Veerstraat 9 Country, P.O. Box 3421, Curacao                             |
| Headquarters                       | Abraham de Veerstraat 9 Country, P.O. Box 3421, Curacao                             |
| Contact Details                    | <a href="mailto:support@citobet.com">support@citobet.com</a>                        |
| Website                            | <a href="https://www.citobet.com/sportsbook">https://www.citobet.com/sportsbook</a> |

## Definitions

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Account            | A registered player profile on the Company's gaming platform, used to access gaming services through the official and licensed gaming website of the Company, hold balances, and conduct transactions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| AML/CFT            | Anti-Money Laundering and Countering the Financing of Terrorism                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Compliance Officer | The designated senior executive at management level responsible for overseeing a Company's compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) laws and regulations. Appointed under Section V.3 of the Regulation, the CO serves as the Company's central point of contact for handling reported suspicions of money laundering or terrorist financing from employees and partners. Their duties include developing, implementing, and maintaining the Company's Internal Policies and Procedures related to AML/CFT, ensuring their effective application across the organization, and continuously monitoring compliance to mitigate financial crime risks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Apostille          | An Apostille is a certificate issued by a designated authority in a country where the Hague Convention Abolishing the Requirement for Legalization of Foreign Public Documents, Apostille Convention, is in force. Apostilles authenticate the seals and signatures of officials on public documents such as birth certificates, notarial, court orders, or any other document issued by a public authority so that they can be recognized in foreign countries that are parties to the Convention.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Beneficial Owner   | <p>Means any natural person(s) owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:</p> <ul style="list-style-type: none"><li>i. In case of natural persons: person, if any on whose behalf the transaction/operation is being carried out.</li><li>ii. In the case of corporate entities: A natural person who ultimately owns or exercises control, directly or indirectly, over a legal entity through a sufficient proportion of its shares or voting rights—except for public limited liability companies listed on regulated markets subject to transparency requirements regarding shareholder and Board of Directors disclosures. A sufficient proportion is generally considered to be ownership of 25% plus one share, whether held directly or indirectly, in the Customer's equity.</li></ul> <p>Exceptional rule – a natural person holding a senior executive position in a Customer which is a legal entity if no person specified in clause (ii) above has been identified or if there is any doubt that the person who has been identified is the beneficial owner.</p> |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <p>iii. In the case of Trust:</p> <ul style="list-style-type: none"> <li>• The settlor;</li> <li>• The trustee(s);</li> <li>• The beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;</li> <li>• The protector, if any;</li> <li>• Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;</li> </ul> <p>iv. In the case of legal arrangements similar to trusts, the natural person holding equivalent or similar position to those referred to in point (iii).</p>                                                                                                                                                                                                                                                                                                                                                                                         |
| BoD                    | The Board of Directors of the Company.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Company                | Means the Green Point Technologies NV                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Customer               | <ul style="list-style-type: none"> <li>• Any person or entity that maintains an account with the Company.</li> <li>• Any person or entity on whose behalf an account is maintained by the Company.</li> <li>• Beneficiaries of transactions who maintain an account with the Company.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CFATF                  | The Caribbean Financial Action Taskforce. An organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| CGA                    | The Curacao Gaming Control Board or the "Regulator".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Regulation             | Regulations for combating of ML/TF and Proliferation of weapons of mass destruction of the Curacao Gaming Control Board of January 2025.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| FATF                   | Means the Financial Action Task Force. An inter-governmental body, the objectives of which are to set standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. It has developed a series of Recommendations that are recognized as the international benchmark for combating money laundering and the financing of terrorism, which form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field. FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques, and promotes the adoption and implementation of appropriate measures globally including countermeasures. In collaboration with other international stakeholders, FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse |
| Financial Transactions | Means deposits and withdrawals through the Account (bonusses are not included).<br>*Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Manual                 | This AML Manual                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ML/TF                  | Money Laundering and Terrorist Financing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| FIU                    | The Financial Intelligence Unit of Curacao "Meldpunt Ongebruikelijke Transacties Curaçao" (MOT Curaçao)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Obligated Entities     | <p>a) Credit Institutions;</p> <p>b) Financial Institutions;</p> <p>c) Electronic Money Institutions;</p> <p>d) Any of the following natural or legal persons in the exercise of their professional activities:</p> <p>I. Auditor, external accountant, tax advisor;</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              | <p>II. Independent legal professional when it participates whether acting on behalf of a client in a financial or real estate transaction, or by assisting in the planning or carrying out of a transaction for its client concerning the:</p> <ol style="list-style-type: none"> <li>1) Buying and selling of real property or business entities;</li> <li>2) Managing of client money, securities or other assets;</li> <li>3) Opening or management of bank, savings or securities accounts;</li> <li>4) Organization of contributions necessary for the creation, operation and management of companies;</li> <li>5) Creation, operation or management of trust, companies, foundations or similar structures;</li> </ol> <p>e) Natural or legal person not covered under paragraph (d) offering the following services:</p> <ol style="list-style-type: none"> <li>I. Formation of companies and other legal persons;</li> <li>II. Acting or, arranging for another person to act as, a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;</li> <li>III. Providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement;</li> <li>IV. Acting or arranging for another person to act as, a trustee, or a trustee of express trust or a similar legal arrangement;</li> <li>V. Holding the shareholding capital of corporate entities and registering such shareholder in the respective registered shareholders on behalf of or on account of third parties, other than a company listed on a regulated market that is subject to disclosure requirements, or ensures that other person exercises respective duties;</li> <li>VI. Any of the services or activities specified in section 4 of the Regulation of Administrative Service Providers and Related Issued Law.</li> </ol> <ol style="list-style-type: none"> <li>f) Real Estate Agents;</li> <li>g) Casinos including online gambling/iGaming services providers;</li> <li>h) Crypto Assets Service Providers;</li> <li>i) Art Dealers and dealers of precious metals, stones, and gems when transacting in cash for transactions exceeding 10.000 EUR.</li> </ol> |
| Online Games | Sports betting, esports-betting, fantasy sports, lottery and bingo, skill-based games and virtual sports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| PEPs         | <p>Means Politically Exposed Person, who is or who has been entrusted with prominent public functions either domestically, either in a foreign country, either by an International Organization (EU, UN, NATO, IMF, etc.), or their close family members and close associates.</p> <p>Close family members include a spouse, a person with whom partnership has been registered, parents, children and children's spouses, and persons with whom children have registered partnership.</p> <p>Close associate includes (i) a natural person who, together with a person who performs or has performed Prominent Public Functions, is the participant of the same</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <p>legal entity or the organization without the status of legal entity or maintains other business relations; or (ii) a natural person who is the only Beneficial Owner of a legal entity or an organization without the status of legal entity that is established or operating de facto with a view to receive economic gain or other personal benefits for a person who performs or performed Prominent Public Functions.</p> <p>Prominent public functions cover:</p> <ol style="list-style-type: none"> <li>1. Heads of State, heads of government, ministers and deputy or assistant minister;</li> <li>2. members of parliament or of similar legislative bodies;</li> <li>3. members of the governing bodies of political parties;</li> <li>4. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;</li> <li>5. members of courts of auditors or of the Boards of Central Banks;</li> <li>6. ambassadors, chargés d'affaires and high-ranking officers in the armed forces;</li> <li>7. members of the administrative, management or supervisory bodies of State-owned enterprises;</li> <li>8. directors, deputy directors and members of the Board or equivalent function of an international organization;</li> <li>9. mayor.</li> </ol> |
| Qualifying Holding     | Means a direct or indirect holding in a customer that represents 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Senior Management      | Means an officer or employee with sufficient knowledge of the Company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Source of Funds        | Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Source of Wealth       | Source of wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Suspicious Transaction | A transaction that deviates from a customer's known, legitimate business or personal activities, or from the expected patterns of transactions for that customer type or account.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Tipping Off            | Means the disclosure to the customer concerned or a third party that information or other relevant material regarding knowledge or suspicion of money laundering has been submitted or will be submitted to FIU, or a disclosure that may impede or prejudice the interrogation and investigation carried out in respect of prescribed offenses or the ascertainment of proceeds, knowing or suspecting that the said interrogation and investigation are taking place.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| TCSPs                  | <p>Trust and Company Service Providers, commonly known as Fiduciary Service Providers, means businesses or individuals engaged in offering services related to the formation, administration, operation, and management of legal persons or arrangements. These services include, but are not limited to:</p> <ul style="list-style-type: none"> <li>• Acting as, or arranging for another person to act as, a director or secretary of a company;</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|  |                                                                                                                                                                                                                                                                                                                                                                          |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"><li>• Providing a registered office, business address, correspondence address, or administrative address for a company;</li><li>• Acting as, or arranging for another person to act as, a nominee shareholder for a company; and</li><li>• Serving as a trustee of an express trust or providing similar fiduciary services.</li></ul> |
|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Contents

|       |                                                          |    |
|-------|----------------------------------------------------------|----|
| 1.    | General Provisions.....                                  | 9  |
| 1.1.  | Policy Statement .....                                   | 9  |
| 1.2.  | Company Information .....                                | 9  |
| 1.3.  | Money-Laundering and Terrorist Financing.....            | 10 |
| 1.4.  | Proliferation Financing .....                            | 10 |
| 2.    | Risk-based Approach and Risk Categorization .....        | 11 |
| 2.1.  | Risk Ratings .....                                       | 11 |
| 3.    | Customers Due Diligence .....                            | 13 |
| 3.1.  | Acceptable form of documents/data.....                   | 15 |
| 3.2.  | Natural Persons .....                                    | 15 |
| 3.3.  | PEPs.....                                                | 16 |
| 3.4.  | High Risk Countries .....                                | 16 |
| 4.    | Periodic Review Process .....                            | 17 |
| 4.1.  | Customer Due Diligence (CDD) Requirements.....           | 17 |
| 4.2.  | Documentation and Record-Keeping.....                    | 17 |
| 4.3.  | Periodic Reviews in Response to Material Changes .....   | 17 |
| 5.    | Transactions Monitoring and Transactions Screening ..... | 18 |
| 5.1.  | Live Transaction Monitoring Process .....                | 18 |
| 5.2.  | Live Transaction Monitoring Triggers .....               | 18 |
| 5.3.  | Post Transaction Monitoring Alert System .....           | 18 |
| 6.    | Screenings .....                                         | 19 |
| 7.    | Termination of Business Relationship .....               | 20 |
| 8.    | Customer Records .....                                   | 20 |
| 8.1.  | Record Keeping .....                                     | 20 |
| 9.    | SARs/Report to the FIU .....                             | 20 |
| 9.1.  | Examples of Suspicious Transactions related to ML .....  | 20 |
| 9.2.  | Reporting of Suspicious Transactions/Activities .....    | 21 |
| 10.   | Board of Directors.....                                  | 21 |
| 11.   | Compliance Function.....                                 | 22 |
| 12.   | Audit Function.....                                      | 23 |
| 13.   | Employee Training Program .....                          | 24 |
| 13.1. | Employees Obligations.....                               | 24 |
| 13.2. | Communication with Employees .....                       | 24 |
| 13.3. | Education and Training .....                             | 24 |
| 13.4. | Training Objectives.....                                 | 24 |
| 13.5. | Training Audience Breakdown .....                        | 24 |
| 14.   | Review and Update.....                                   | 26 |

# 1. General Provisions

## 1.1. Policy Statement

Under the mandate of the CGA the Company is required to maintain a comprehensive, written AML Policy that sets out the measures adopted for the prevention of money laundering (ML), terrorist financing (TF), and the protection of the Company's reputation, operations, and financial integrity.

The Company's risk management framework is designed to proactively identify, assess, and mitigate ML/TF risks. Risk-based controls are applied from the outset—prior to the onboarding of any customer or business relationship—and are maintained and adapted throughout the duration of the relationship to ensure ongoing compliance.

This Manual sets forth the policies, procedures, and internal controls that ensure full adherence by all employees, officers, and relevant stakeholders to the applicable AML/CFT legislation and regulatory framework, both locally and internationally.

The purpose of this AML Manual is to:

- Combat money laundering, terrorist financing, and proliferation financing;
- Implement international best practices and industry standards;
- Promote enterprise-wide compliance with the AML/CFT legal and regulatory framework;
- Provide a structured and consistent methodology for managing risks associated with customers, products, services, delivery channels, jurisdictions, and payment mechanisms.

The design, implementation, and ongoing monitoring of the AML framework is the responsibility of the Board of Directors of Green Point Technology NV., who formally approve this Manual. The Manual is subject to a minimum annual review, and may be amended more frequently to reflect material changes in the AML/CFT legislative framework, regulatory guidance, internal audit recommendations, or operational risk exposure. The Compliance Officer (CO) is authorized to propose urgent updates arising from internal findings or third-party audit outcomes.

This AML Manual reflects the key objectives and obligations under Curaçao's AML/CFT legal framework, as well as the expectations of the Regulator and relevant international standard-setting bodies. The Company's directors, officers, employees, and appointed third-party consultants are fully committed to upholding the standards and responsibilities established herein. This Manual applies to all personnel at all levels within the Company, as well as any external parties engaged for audit, compliance, or support functions.

## 1.2. Company Information

Green Point Technology N.V. is a company registered in Curaçao under registration number 163399, with its principal office located at Abraham de Veerstraat 9 Country, P.O. Box 3421, Curaçao. The Company operates as an online casino and holds license number OGL/2024/256/0304, issued by the Curaçao Gaming Control Board (CGA). The Company is duly authorized and regulated by the CGA to offer business-to-consumer (B2C) remote gaming services, including games of chance and sports betting, through its approved domain: <https://www.citobet.com/sportsbook>.

The Company conducts its business operations from its headquarters in Curaçao and maintains full compliance with the licensing requirements and regulatory conditions imposed by the CGA. In accordance with such conditions, the Company is prohibited from offering its services to users located in restricted jurisdictions, including but not limited to the United States, Australia, Curaçao, France, Germany, Austria, Spain, Iran, Iraq, the United Kingdom, and the Netherlands.

The Company strictly adheres to these territorial restrictions and does not target, promote, solicit, or provide services to individuals in jurisdictions where online gambling is prohibited.

### 1.3. Money-Laundering and Terrorist Financing

Money laundering is considered to be when the following are conducted intentionally:

- a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;
- c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
- d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points (a), (b) and (c).

Terrorist financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they are used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offenses described in Penal Code on combating terrorism, criminal activities generating such proceeds include:

- a) Attacks upon a person's life or physical integrity;
- b) Kidnapping or hostage-taking;
- c) Causing extensive destruction to a government or public facility, infrastructure, public place, or private property likely to endanger human life or result in major economic loss;
- d) Seizure of aircraft, ships, or other means of public or goods transport;
- e) Manufacture, possession, acquisition, transport, supply, or use of weapons or explosives, including nuclear, biological, or chemical weapons;
- f) Release of dangerous substances, or causing fires, floods, or explosions endangering human life;
- g) Interfering with or disrupting the supply of water, power, or other fundamental natural resources, endangering human life;
- h) Illegal system interference, seriously hindering or interrupting information systems;
- i) Threatening to commit any of the acts listed in points (a) to (h).

The aims referred above are:

- a. Seriously intimidating a population;
- b. Unduly compelling a government or an international organization to perform or abstain from performing any act;
- c. Seriously destabilizing or destroying the fundamental political constitutional economic or social structure of a country or an international organization.

It is noted that directing a terrorist group or participating in the activities of terrorist group including information or material resources or by funding its activities in any way (e.g. paying for the rent or for the food of the terrorists), with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group, it is considered an offence relating to terrorist activity.

### 1.4. Proliferation Financing

The Company recognizes the critical importance of addressing Proliferation Financing (PF), which involves the use of financial resources to support the development, acquisition, transfer, or delivery of weapons of mass destruction (WMD) and their associated delivery systems.

The company adheres strictly to international sanctions regimes, including those enforced by the United Nations Security Council and the European Union, as well as Curaçao's national legislative requirements under the Sanctions National Ordinance (SNO) and the Kingdom Sanction Act. Transactions and counterparties are routinely screened against relevant sanctions lists to ensure compliance and prevent any financial interaction that could facilitate WMD proliferation.

## 2. Risk-based Approach and Risk Categorization

The Company adopts a Risk-Based Approach (“RBA”) for its assessments to ensure that resources are allocated effectively, prioritizing areas with the highest risk exposure. The RBA ensures that the most significant risks receive the highest level of attention, allowing the Company to focus its efforts where they are needed most.

The Company takes a holistic view of the risk factors identified above that, together, determine the level of ML/TF risk associated with a business relationship.

As part of the assessment, the Company weighs risk factors differently, depending on their relative importance. When weighing risk factors, the Company makes an informed judgment about the relevance of different risk factors in the context of the business relationship. Ultimately, the weight given to each factor varies from product to product and customer to customer. When weighing risk factors, the Company ensures the following:

- a) Weighting is not unduly influenced by one factor only;
- b) Economic or profit considerations do not influence the risk rating;
- c) Weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk; and
- d) The situations that always present a high Money Laundering risk or even prohibited engagement with the customer cannot be overruled by the weighting.

The Company categorizes clients into three risk levels: **a) Low, b) Medium, and c) High**. This classification is determined by a dynamic risk matrix using a semi-auto dynamic Excel Spreadsheet evaluating factors such as client type, domicile, primary countries of operation, years in business, relevant licenses, business activities, and the complexity and transparency of corporate structures.

Additional considerations include annual credit turnover, assessments of transactional and economic profiles, Company services provided, adverse media findings that may prompt further investigation, and sanctions/ PEP screening results. The risk classification also accounts for the nationalities and permanent residencies as well for the economic profile of all identified persons with significant control.

### 2.1. Risk Ratings

The **Client Acceptance Policy (‘CAP’)** defines client acceptance categories at the Company, specifying **prohibited client types and those that, if accepted, must be classified at a minimum as High risk**. Clients not falling into prohibited or high-risk types are categorized based on the dynamic Client Risk Matrix (semi-auto dynamic Excel Spreadsheet). However, ***acceptance is not guaranteed***, as any client may still be rejected following an assessment by the CO.

The Client Risk Matrix is a dynamic semi-auto Excel Spreadsheet, risk-based evaluation tool used by the Company to determine the appropriate risk categorization of each customer. The matrix is designed in accordance with the **Risk Factor Guidelines** and considers the following risk categories: **Customer Risk, Geographical Risk, Product, Service and Transaction Risk, and Delivery Channel Risk**.

#### Customer Risk:

- **Legal form and entity type** of the customer;
- **Nature and sector of the customer's business activities**, with particular attention to any involvement in **business sectors classified as prohibited** under the Company’s Client Acceptance Policy;
- **Complexity and transparency** of the ownership and control structure;
- Presence of elements that may **facilitate anonymity**, such as the use of bearer shares, nominee shareholders, or trust arrangements;
- Evaluation of the **economic rationale** behind recent changes in shareholding;
- Whether the customer or its **UBO** appears on any **Sanctions List, PEP List**, or has been subject to **adverse media**;

- Quality and traceability of the declared **Source of Funds and Source of Wealth** of the customer and customer's UBO, including links to any **high-risk economic sectors**.

#### Product, Service Risk and Transactions Risk:

This dimension analyses how the nature of the services requested and expected transactional behavior may expose the Company to increased risk. The following indicators are taken into account:

- In-game spend vs. deposit behavior
- Use of multiple accounts or devices
- Structured or anomalous deposit patterns
- Use of third-party payment methods
- Jurisdictional risk of player residence
- Unusual or withdrawal-focused behavior
- Internal value transfer mechanisms (e.g., tokens)
- High-velocity deposit–withdrawal cycles without gaming activity

#### Geographic Risk:

This category evaluates the customer's exposure to jurisdictions associated with elevated ML/TF risk. The matrix considers:

- **Country of residence** of the customer or the UBOs;
- **Primary jurisdictions of business operations;**
- **Countries from which the customer expects to send or receive funds;**
- Whether the jurisdictions in question are subject to **EU high-risk third country and FATF listings, sanctions, or strategic AML/CFT deficiencies**.

#### Delivery Channels Risk Factors

The present Risk Factor analyzes the potential risk that may arise from the delivery channels that the Company is using to deliver its products and services to its customers, such as:

- Direct leads from Affiliates;
- Non-Face to Face customers.

#### Risk Scoring and Overrides

Each risk factor is assigned a score based on predefined weightings. The cumulative score determines the overall risk categorization of the client as **Low**, **Medium**, or **High**.

#### **Update Frequency**

- Updates are made whenever the CAP or the predefined lists (FATF, EU, sanctions, etc.) are revised. CAP provisions that the country list is Subject to amendment at any time by the CO to align with changes to the EU, UN, OFAC or local sanctions lists, or changes to the EU lists of High-Risk Third Countries and EU Non-Cooperative for Tax Purposes, or the FATF's Grey and Black Lists.
- An annual review is conducted by the CO to ensure ongoing compliance if no updates occur in the interim.

### 3. Customers Due Diligence

Client due diligence is triggered when:

- Transactions Equal to or Exceeding NAF 4,000:
- For any transaction involving an amount of NAF 4,000 or more, whether conducted as a single event or a series of linked transactions,
- Occasional transactions that exceed NAF 4,000 threshold, even if the customer does not maintain an ongoing relationship with the company
- Linked Transactions Exceeding NAF 4,000: Even if individual transactions fall below the NAF 4,000 threshold, the company assesses whether multiple linked transactions cumulatively exceed this amount.
- When there are doubts about the veracity or adequacy of previously obtained customer identification data;
- When there are material changes in the due diligence documentation maintained in the client's folder;
- During the course of the business relationship to ensure that the client's folder remains up to date;
- When there is a suspicion of ML/TF regardless of any derogation, exemption, or threshold.

Irrespective of the client's risk categorization, the following due diligence measures shall always be undertaken:

- Identification of the customer and verification of their identity on the basis of documents, data, or information obtained from a reliable and independent source;
- Where applicable, identification of the beneficial owner and verification of their identity to ensure that the Company knows who the beneficial owner is;
- Establishing the purpose and intended nature of the business relationship;
- Collection of additional relevant information such as:
  - Expected turnover;
  - Country and address of residence of the client, and UBOs;
  - Destination of payments and main jurisdictions of counterparty banks;
  - Business details;
  - PEP status of the customer and associated persons;
  - Expected annual credit turnover.
- Conducting ongoing monitoring of the business relationship, including scrutiny of transactions, to ensure consistency with the company's knowledge of the customer and risk profile.

#### Proactive CDD Measures at Onboarding

The Company emphasizes early completion of CDD. Identity checks are conducted at the point of registration, regardless of financial thresholds. This pre-emptive strategy is intended to prevent the entry of illicit funds into the system by ensuring that no user is granted full platform access without having first undergone due diligence.

#### Operational Limits for Incomplete CDD

- In situations where a player reaches the NAF 4,000 threshold prior to completing CDD, specific

limitations are imposed:

- If triggered by a deposit: Further deposits and withdrawals are restricted; however, the customer may continue to participate in gaming using their current account balance.

If triggered by a withdrawal request: The player's account is temporarily frozen, and all gameplay is suspended until full verification is completed.

If a customer fails to submit the required documentation within 30 days after reaching the transaction threshold, the following measures are taken:

- The business relationship is terminated;
- If there are grounds for suspicion of ML or TF, a Suspicious Transaction Report (STR) is filed with the Financial Intelligence Unit (FIU);
- In the absence of suspicion, any remaining funds are returned to the source of deposit (e.g., the original bank account or digital wallet);
- Where suspicion persists, internal policies determine whether funds should be frozen pending further investigation, ensuring compliance with applicable law.

### 3.1. Acceptable form of documents/data

Information, data, and documents will be accepted when issued by:

- I. The relevant state authorities empowered to issue identification documents such as Passports, National IDs, Driving Licenses;

### 3.2. Natural Persons

The true identity of natural persons must be ascertained by obtaining the following information:

- Full legal name as stated on the official identity card or passport;
- Issuing date, expiry date, and issuing country of the identity card or passport;
- Nationality\*;
- Date of birth;
- Place of birth
- Full permanent address including postal code;
- Contact details;

\*If a customer holds multiple nationalities, the Company shall obtain comprehensive information on all nationalities held, along with a clarification regarding the circumstances of the customer's multi-citizenship status.

Verification of information obtained is required via:

- A valid identity card or passport;
- A recent (up to six months old) utility bill, tax bill, or bank statement. Utility bills must demonstrate the existence of immovable property i.e. electricity, water, sewage, gas, bills, fixed telephone lines, internet home, municipality taxes, etc. **Mobile bills are not accepted.**
- Documentation evidencing source of income and wealth – ***\*Applicable to Customers and individuals identified as UBOs which are classified as High Risk.***

The onboarding and identity verification process for players is fully automated and conducted through the Company's authorized and licensed gaming domain.

The onboarding process comprises the following steps:

#### 1. Document Submission

Prospective clients are required to upload an official identification document (e.g., passport, national identity card, or driving license);

#### 2. Background Screening

The customer is screened through the LexisNexis platform against databases covering PEPs, sanctions, and adverse media.

#### 3. Liveness Detection and Facial Match

A liveness check is performed to ensure the presence of a real individual during the process by requesting a real time selfie. The uploaded selfie is matched against the photograph on the identification document, with a facial match score provided to verify authenticity. ***\*Applicable to Customers and individuals identified as UBOs which are classified as High Risk.***

#### 4. IP Geo-Location ***\*Applicable to Customers which are classified as High Risk.***

The Company employs IP geo-location verification tools to monitor and assess the geographic origin of user access in real time. These tools are used to:

- **Verify that players are not accessing the platform from prohibited or high-risk jurisdictions;**
- **Detect the use of VPNs, proxies, or anonymization services intended to obscure the user's true location and bypass territorial restrictions;**
- **Identify mismatches between registered account details and actual access location, which may indicate the use of stolen credentials, third-party access, or other forms of unauthorized account activity.**

#### 5. First Deposit Rule

The Company requires that a player's initial deposit be made through a payment institution regulated in a jurisdiction recognized as having a robust and effective AML/CTF framework. **\*Applicable to Customers which are classified as High Risk.**

#### 6. Identity Verification

These combined measures ensure that the Company verifies the true identity of the client, preventing the onboarding of individuals using fictitious identities or attempting to act anonymously.

### 3.3. PEPs

Concerning identifying during the onboarding process whether a customer is a PEP, the Company:

- Uses LexisNexis database that checks against Global databases of PEP lists.

Once a customer is identified as a PEP the customer is classified as **high risk** and the following due diligence measures shall be applied:

- The Company shall take adequate measures to establish the source of wealth and the source of funds to be used in the business relationship in order to ensure that it will not handle the proceeds of corruption or other criminal activity. The Company will verify the source of wealth and funds on the basis of reliable and independent data, documents, or information;
- The establishment of the business relationship requires approval from the Senior Management. For the ongoing continuation of the relationship, approval from the CO is necessary;
- The Company will conduct enhanced ongoing monitoring of transactions until the PEP status of the customer changes.

The accounts of PEPs shall be subject to ongoing monitoring. At least an **annual review** shall be performed in order to determine whether to allow the continuance of operation. The report shall be submitted for consideration and approval to the **CO** and filed in the customer's file.

The Company shall ensure that a customer's due diligence information is kept up to date, as existing customers may sometimes become PEPs after the establishment of the business relationship. As part of this process, the Company will perform regular re-screenings via LexisNexis to identify whether a PEP customer maintains his PEP status or whether the status of a non-PEP customer has changed.

In a case that a PEP is no longer entrusted with a prominent public function by a Member State or a third country, or with a prominent public function by an international organization, the Company shall, for at least 12 months, take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to PEPs.

The Company shall maintain a PEP's registry, which shall include the relevant details of the PEP with whom a business relationship has been established or rejected.

### 3.4. High Risk Countries

With respect to business relationships or transactions involving high-risk third countries, the Company will apply the following enhanced customer due diligence measures:

- Obtain additional information on the customer, the beneficial owner(s), and the intended nature of the business relationship, clarifying the connection with the high-risk jurisdiction(s) in question, and verifying the business rationale behind this connection;

- b) Obtain information on the source of funds and source of wealth of the customer and of the beneficial owner(s);
- c) Obtain information on the reasons for the intended or performed transactions with the high-risk jurisdiction(s), verifying whether there are legitimate reasons for such transactions;
- d) Obtain the approval of Senior Management for establishing or continuing the business relationship;
- e) Transactions involving high-risk countries are reviewed before execution, regardless of the amount.

The enhanced due diligence measures outlined in this section shall be applied to mitigate associated risks.

## 4. Periodic Review Process

The periodic review procedure provides guidance on the process of conducting scheduled compliance reviews for Clients based on their risk classification, ensuring adherence to Anti-Money Laundering (AML) regulations and internal policies.

Periodic compliance reviews are performed based on Client's risk classification as per the AML Manual:

- **High Risk** – Every **12** months
- **Medium Risk** – Every **24** months
- **Low Risk** – Every **36** months

Steps to be undertaken during a periodic review:

1. **Reviewing of the transactions of the client** to ensure that the transactional behavior of the client aligns with the economic profile of the subject client and to identify any deviations/
2. **Review Existing Documentation and Information** – Evaluate the client's economic profile, and the validity of current KYC documents in the client's folder.
3. **Conduct Screening of the Client** using the following sources:
  - LexisNexis;
  - Google News & open-source media checks;
4. **Escalate Screening Findings** – Report any adverse media, PEP status, or other risk indicators to the CO.
5. **Verify Customer Due Diligence (CDD) Compliance** – Confirm that all required CDD documents are in order, valid, up to date, and all information and documentation collected aligns with the expected economic profile of the client.
6. **Maintain Detailed Records** – Document results and analysis performed, and update accordingly the client's economic profile.

### 4.1. Customer Due Diligence (CDD) Requirements

Basic CDD requirements for periodic reviews are as follows:

- Recent utility bills (issued within the last six months) and renewed passports (if expired) for Customers, and UBO(s).;
- In case of clients classified as high risk, recent documentation to verify the customers or the UBO's source of wealth and active income (e.g., tax forms, pay slips, contracts, rental agreements, dividend certificates).

### 4.2. Documentation and Record-Keeping

The results of the periodic review must be documented in the client's economic profile, with all collected documentation properly saved and organized in the client's folder. The next review date must be updated in both the client's profile and the CRM.

### 4.3. Periodic Reviews in Response to Material Changes

In addition to scheduled periodic reviews, whose frequency is determined by the client's risk rating, the Compliance team may initiate a periodic review in response to material changes in the customer's situation, legal status, or behavior.

**Examples** of such material events include:

1. A transaction which appears to be unusual and/or significant compared to the normal pattern of transactions, the business activity and the economic profile of the customer.
2. Transactions equal to or exceeding Naf. 4,000, whether executed as a single transaction or as multiple smaller transactions that appear to be linked.
3. Significant change in the situation of the customer such as:
  - Expiration of Identification Document;
  - Sanctions/PEP/ Adverse Media Match;
  - Change of the risk level of the customer (e.g. customer from lower to higher risk).
4. Significant change in the way and rules of the operation of the account, such as:
  - Activation of a dormant account.
  - Significant changes in the volume or pattern of transactional activity associated with the account.

## 5. Transactions Monitoring and Transactions Screening

Transaction monitoring is a critical component of Company's AML framework. It involves the systematic review and analysis of transactions to identify suspicious activities related to money laundering, terrorist financing, or other illicit behavior. This process includes analyzing transaction patterns, detecting anomalies based on predefined rules and thresholds, and ensuring compliance with regulatory requirements.

The Compliance Department, manages the daily clearance of compliance alerts and triggers raised by the live transaction monitoring system.

### 5.1. Live Transaction Monitoring Process

Live transaction monitoring operates through a centralized clearing system designed to detect and flag potentially suspicious transactions in real time. This system incorporates compliance triggers that enable immediate intervention when necessary.

### 5.2. Live Transaction Monitoring Triggers

Triggers for live transaction monitoring include:

- **High-value transactions:** Single transactions equal to or exceeding Naf 4.000.
- **High-risk jurisdictions:** Transactions originating from or sent to countries classified as high risk in line with the Customer Acceptance Policy.
- **Prohibited jurisdictions:** Transactions originating from or sent to countries classified as prohibited in line with the Customer Acceptance Policy.
- **Negative findings:** Transactions flagged through our screening tools for PEP, Sanctions, or Adverse Media.

### 5.3. Post Transaction Monitoring Alert System

Post-transaction monitoring is a critical procedure within the transaction monitoring unit of the Company. Its purpose is to provide an additional layer of scrutiny for transactions that were not captured during the live transaction monitoring process. The analysis of these transactions, particularly those that did not initially raise alerts, helps the company identify unusual patterns, such as aggregation anomalies and significant turnovers that were not previously flagged. Consequently, the post-transaction monitoring enhances Company's overall AML framework and ensures consistency with the customer's declared activities. The post-transaction monitoring process is guided by two key rules, **Aggregation Alerts** and **Turnover Alerts**.

- a) **Aggregation Alerts:** These alerts are generated when the total value of transactions through an account exceeds a predefined threshold within a one-week period. This mechanism facilitates the detection of potential structuring activities or high-risk transactional relationships that need further examination;
- b) **Turnover Alerts:** These alerts are triggered when a customer's credit turnover exceeds a predefined threshold over a monthly period. Significant variances in the customer's activities may suggest a reevaluation of the customer's profile.

## 6. Screenings

Screening is performed on all customers. Screening tools used:

- LexisNexis;
- Google News & Open-Source Media Checks;

If any high-risk factors are identified, the alerts are escalated to the CO for further investigation and final assessment.

### Assessment of Adverse Media

To evaluate the credibility and materiality of adverse media findings, the responsible officer shall consider the following key factors:

1. **Source Reliability** – The reliability of the media source shall be assessed, with preference given to **reputable international news agencies, national newspapers, and publications with established editorial oversight**. Media sources that lack editorial control, such as certain social media platforms, blogs, and non-verified sources, may be deemed less credible.
2. **Content Relevance** – It is essential to determine whether the adverse media directly relates to **financial crime risks**. Not all negative information is relevant; for instance, minor infractions, such as traffic violations, do not impact the Company's risk assessment.
3. **Contextual Analysis** – The **context** of the negative media report shall be evaluated, including **the jurisdiction in which the event occurred, the subject's public profile, and the timing of the report**, as these factors may influence the materiality of the findings.<sup>z</sup>

### Decision-Making Process

Following the assessment, the responsible officer shall determine whether the findings **constitute a predicate money laundering (ML) offense** in accordance with the provisions of the Criminal Code (NG 2011 no. 48)

- If the subject has been **convicted of a predicate ML offense**, the application shall be **rejected**.
- If the adverse media relates to **minor offenses**, the CO shall evaluate the circumstances on a **case-by-case basis** and determine whether additional risk mitigation measures are required.

The CO's **assessment and final determination must be fully documented in the customer's file**. While the Company **does not impose a blanket restriction** on onboarding individuals convicted of minor offenses, or connected to adverse media, such customers may be **classified as high-risk under the Risk-Based Approach (RBA)**. This classification ensures that the **customer's transactions are subject to enhanced scrutiny** throughout the business relationship.

## 7. Termination of Business Relationship

The CO may recommend the termination of any business relationship if changes in circumstances lead to an excessively high ML/TF risk.

Notwithstanding the foregoing, the CO may initiate the termination of a business relationship if a client is dormant, unresponsive to periodic reviews or other compliance requests.

## 8. Customer Records

### 8.1. Record Keeping

The Company shall retain the following documents and information for a period of **five (5) years** after the termination of the business relationship or the execution of an occasional transaction:

- a) Customer due diligence documentation and information necessary to comply with the requirements outlined in this Manual;
- b) Supporting evidence and transaction records necessary for determining and reconstructing transactions; and
- c) Relevant documents regarding correspondence with customers and other persons with whom the Company maintains a business relationship.

This retention ensures that authorities can reconstruct financial transactions and facilitate investigations into potential money laundering (ML) or terrorist financing (TF) offenses.

In alignment with applicable regulatory requirements and the Company's data retention policy, these records shall be retained for an **additional five (5) years** to support financial audits, regulatory reviews, and risk management processes.

**After the ten-year period, records shall be securely deleted unless further retention is required by law or ongoing proceedings.**

All retained documents shall be made available without delay to the relevant competent authority upon request, in compliance with applicable legal and regulatory obligations.

## 9. SARs/Report to the FIU

### 9.1. Examples of Suspicious Transactions related to ML

The employees of the Company should be able to detect any unusual or suspicious transactions or activities that are inconsistent with the economic profile of the customer and report their suspicion to the CO of the Company.

Suspicious transactions/activities include, but are not limited to, the following:

- a) Transactions without clear economic purpose or unnecessarily complex transactions;
- b) Transactions or the size of transactions requested by the customer do not comply with their normal practice and business activities;
- c) Large volume of transactions and/or money deposited or credited into, an account when the nature of the customer's business activities would not appear to justify such activity;
- d) Any transaction the nature, volume, or frequency appears to be unusual;
- e) Transactions that are inconsistent with normal market practice, in relation to the size of the order and the frequency;
- f) Settlement of the transaction by a third person who is different than the customer;
- g) Instructions of payment to a third person who has no obvious link/connection with the instructor;
- h) Transfer of funds to and from countries or geographical areas that do not apply, or that apply inadequately FATF's recommendations on ML/TF. The customer is unwilling to provide complete information when establishing a business relationship regarding the nature and purpose of its business, and the anticipated account activity. The customer usually gives little or misleading information that is difficult or costly for the company to verify;
- i) Customer gives unusual or suspicious identification documents whose authenticity cannot be directly verified;
- j) Unexplained inconsistencies arising during the customer identification (e.g., regarding previous or current country of residence, country of issue of the passport, and documents furnished to confirm name, address, and date of birth etc.);
- k) Any transaction that has already been submitted to law enforcement, such as the Police or the Department of Justice, for its suspected connection to money laundering (ML) or terrorist financing (TF) is classified as unusual by default.

- l) Any transaction carried out by or on behalf of individuals, legal entities, or organizations listed under the Sanctions National Ordinance (N.G. 2014 no. 55), or appearing on other official sanction lists, is deemed unusual.
- m) Changes in performance and behavior of the Company's employees.

## 9.2. Reporting of Suspicious Transactions/Activities

The CO receives information from the Company's employees in relation to knowledge or suspicion of money laundering or terrorist activities and prepares a written report with all relevant information. He will then evaluate the information received and decide whether or not he will submit an official report to FIU. The decision of the CO must be in written form where he fully explains his decision.

If, following the evaluation of the information, the CO decides to notify the FIU, he must do so electronically as described in through the portal GoAML. At the same time all accounts and portfolios of the customer in question are closely monitored and examined.

The CO, although not required, may also contact CGA or any other appropriate law enforcement authority in cases where a reported suspicion may require immediate attention.

The Company and all relevant persons should not disclose (tip-off) to the customer in question that information or other relevant material regarding knowledge or suspicion of money laundering has been submitted to the FIU.

## 10. Board of Directors

It is the responsibility of the Board of Directors (the "BoD") of the Company to appoint the members of the Senior Management and to determine their duties and responsibilities. This includes, among other, ensuring that:

- a) An AML/CFT culture is maintained within the Company;
- b) AML/CFT risk management and regulatory requirements are embedded at all levels of the Company and in all elements of its activities;
- c) Independent reviews and testing on the Company's compliance with its AML/CFT policies are performed;
- d) Regular and timely information is made available to the BoD; and
- e) The Company's staff members are capable of addressing identified AML risks, receiving an appropriate level of AML/CFT training relevant to the role they undertake within the Company (particularly in the area of suspicious activity monitoring and reporting), and establishing whether the training received allows staff members to effectively fulfill their responsibilities.

The BoD is also responsible for the following:

- a) to determine, record and approve the general policy principles of the company in relation to the prevention of ML/TF and communicate them to the AMLCO;
- b) to appoint an AMLCO and, where necessary, assistant AMLCO, and determine their duties and responsibilities, which are recorded in the Manual;
- c) to approve the Manual;
- d) to ensure that all requirements of the Law and of the Directive are applied, and assure that appropriate, effective, and sufficient systems and controls are introduced for achieving the abovementioned requirement;
- e) to assure that the AMLCO and his/her assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of ML/TF, have complete and timely access to all data and information concerning Customers' identity, transactions' documents and other relevant files and information maintained by the company so as to be fully facilitated in the effective execution of their duties, as included herein;
- f) to ensure that all employees are aware of the person who has been assigned the duties of the AMLCO, as well as his assistant, to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to ML/TF;
- g) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the AMLCO, either directly or through his assistants, if any, and notifies accordingly the AMLCO for its explicit prescription in the Manual;
- h) to ensure that the AMLCO has sufficient resources, including competent staff and technological equipment, for the effective discharge of his duties; and
- i) to assess and approve the AMLCO's Annual Report and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report.

## 11. Compliance Function

It is the responsibility of the Company's Board of Directors to appoint an AMLCO, who belongs to the senior management of the Company so as to command the necessary authority, and to determine their duties and responsibilities. In general, the AMLCO is responsible for at least the following:

- a) Designs the internal practice, measures, procedures and controls relevant to the prevention of ML/TF, and describes and explicitly allocates the appropriateness and the limits of responsibility of each department that is involved in the abovementioned;
- b) Develops and establishes the Client Acceptance Policy, and submits it to the BoD for consideration and approval;
- c) Develops and establishes the Company's Risk Matrix, which applies the provisions of the Client Acceptance Policy;
- d) Prepares an AML manual regarding ML/TF;
- e) Monitors and assesses the correct and effective implementation of the policy, the practices, measures, procedures and controls of points (a), (b), and (c) and in general the implementation of the procedures described in the AML Manual of point (d). In this regard, applies appropriate monitoring mechanisms, which will provide him all the necessary information for assessing the level of compliance of the departments and employees of the Company with the procedures and controls which are in force. In the event that he identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures, and controls, gives appropriate guidance for corrective measures and where deems necessary informs the BoD;
- f) Receives information from the Company's employees which is considered to be knowledge or suspicion of ML/TF activities or might be related with such activities. The information may be received in a written report form (the "Internal Suspicion Report");
- g) Evaluates and examines the information received as per point (f), by reference to other relevant information and discusses the circumstances of the case with the informer and, where appropriate, with the informer's superiors. The AMLCO records his findings, evaluation and final assessment in the "Internal Evaluation Report," specifying whether the case should be escalated to the FIU or if alternative mitigating actions should be taken. If the AMLCO decides to notify FIU, then he does so electronically through the web application goAML;
- h) Acts as the first point of contact with the FIU, upon commencement and during an investigation as a result of filing a report to FIU according to point (g);
- i) Acts as the first point of contact and is responsible for regulatory reporting to the CGA;
- j) Ensures the accuracy and maintenance of the lists of customers categorized following a risk-based approach;
- k) Recommends the termination of any business relationship if changes in circumstances result in an excessively high ML/TF risk;
- l) Notwithstanding (k), the AMLCO may initiate the termination of a business relationship or specific product/service if the client is dormant, unresponsive to periodic reviews or compliance requests, or falls outside the risk appetite of the Company, PSP partners, or applicable Scheme Rules;
- m) Prepares and submits the AMLCO Annual Report to the Board of Directors for review and consideration;
- n) Responds to all requests and queries from the FIU and Law Enforcement including those related to the freezing of funds or accounts when required, ensuring full cooperation and the timely provision of all requested information;
- o) Provides the final recommendation to approve or decline all prospective clients onboarded to the Company's corporate segment of the business. Following a risk-based approach, the AMLCO has the authority to manually adjust the risk rating assigned to any client;
- p) As part of Senior Management, grants the final approval to conclude client periodic reviews, including those for high-risk customers;
- q) Maintains a registry which includes the reports of points (g), (h), (m), (n), (o) and (p) above and relevant statistical information;
- r) Ensures that all employees receive as a minimum annual AML/CFT training, while Compliance staff undergo targeted training;
- s) Provides advice and guidance to the employees of the Company on subjects related to ML/TF;

## 12.Audit Function

The Internal Auditor is responsible for reviewing and evaluating, at least on an annual basis, the appropriateness, effectiveness, and adequacy of the policies, practices, measures, procedures, and control mechanisms applied for the prevention of ML/TF. The findings and observations of the internal auditor are submitted, in a written report form, to the BoD which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies which have been detected, following that the Audit Report is submitted to the CGA. In general, the Internal Auditor is responsible for the following:

- a. To establish, implement, and maintain an audit plan to examine and evaluate the adequacy and effectiveness of the Company's systems, internal control mechanisms, and arrangements;
- b. To issue recommendations based on the result of work carried out in accordance with point (a);
- c. To verify compliance with the recommendations referred to in points (b); and
- d. To report in relation to internal audit matters on a frequent basis, and at least annually.

The Internal Auditor is accountable directly to the BoD. All procedures at all levels of the hierarchy of the Company are the object of systematic audit control. Audits are carried out on an annual basis, while extraordinary spot audits are to be carried out without notice.

During investigations and audits, the Internal Auditor has access to all the Company's records, files, and documents and may seek the assistance of any of the Company's employees, who are expected to provide it.

## 13. Employee Training Program

### 13.1. Employees Obligations

The employees of the Company are required to report anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to ML/TF.

An employee who knows or reasonably suspects that a customer is may engaged in the laundering or financing of terrorism offenses, commits an offense if he does not disclose the said information to the CO as soon as it is reasonably practicable after it comes to his attention.

### 13.2. Communication with Employees

The CO shall have regular and on-going communication with all employees as regards issues related to ML/TF. Communication may be performed via emails, face-to-face meetings, and participation in practice group meetings where AML/CFT issues are discussed. The communication of the CO with employees shall primarily aim to:

- a) Inform employees about changes in the regulatory framework as regards AML/CFT;
- b) Assist employees in understanding the procedures followed by the Company to ensure compliance with the regulatory framework;
- c) Identify where any information has been withheld by a staff member about any possible suspicion with respect to ML/TF activities; and
- d) Identify those employees that need further training.

### 13.3. Education and Training

This training plan outlines the compliance training program, segmented by the various roles within the organization. The plan ensures that all employees, especially new recruits, receive timely and relevant training on Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and evolving regulatory requirements, thus fostering a strong culture of compliance.

### 13.4. Training Objectives

- **Enhance knowledge** of AML/CFT obligations, industry standards, and regulatory changes.
- **Strengthen skills** for transaction monitoring, customer onboarding, and compliance reporting.
- **Maintain compliance** with the applicable Directives and legal framework, ensuring that responsibilities are clearly understood across the board.
- **Onboard new hires** effectively, ensuring immediate awareness of AML/CFT policies and procedures.

### 13.5. Training Audience Breakdown

#### Compliance Department

This section covers specialized training for the Compliance Department.

#### Transaction Monitoring

- **Objective:** Ensure expertise in identifying, flagging, and reporting suspicious transactions.
- **Training Frequency:** A minimum of 10 training hours annually.
- **Core Topics:**
  - Transaction monitoring systems and risk indicators
  - Red flags for suspicious activities
  - Regulatory expectations for reporting (e.g., SAR/STR)
  - Updates to sanctions lists and PEP screening
  - Case studies of recent AML breaches and best practices

#### Onboarding

- **Objective:** Maintain high standards for customer onboarding, KYC processes, and verification procedures.

- **Training Frequency:** A minimum of 10 training hours annually.
- **Core Topics:**
  - KYC and Customer Due Diligence (CDD) requirements
  - Enhanced Due Diligence (EDD) for high-risk clients
  - Identification of beneficial ownership
  - Ongoing monitoring of client profiles
  - Legal obligations related to record keeping and reporting

#### **Various AML Matters**

- **Objective:** Ensure deep understanding of the AML framework.
- **Training Frequency:** A minimum of 10 training hours annually.
- **Core Topics:**
  - In-depth understanding of AML/CFT regulations
  - Liaising between departments on AML issues
  - Cross-border compliance concerns and international best practices
  - Preparation of SARs and STRs
  - Practical examples of internal audits and compliance testing

#### **AMLCO (Anti-Money Laundering Compliance Officer)**

- **Objective:** Equip leadership with the necessary tools to oversee the AML compliance framework and ensure effective risk management.
- **Training Frequency:** 20 training hours annually.
- **Core Topics:**
  - AML governance and oversight responsibilities
  - Recent regulatory developments in AML/CFT
  - Risk assessment frameworks and compliance audits
  - Reporting obligations to external regulators
  - Case law, enforcement actions, and best practices
  - Horizon scanning for future legislative changes

#### **Board of Directors**

- **Objective:** Keep the Board informed of their regulatory responsibilities and provide foresight into upcoming regulatory developments.
- **Training Frequency:** Annually, with additional updates on regulatory developments provided quarterly, as applicable.
- **Core Topics:**
  - Board-level responsibilities
  - Recap of regulatory updates from 2024
  - Anticipated changes in legislation and regulatory expectations for 2025

- Supervisory expectations and accountability
- Overview of AML risk management and governance

#### **General AML Training for All Staff**

- **Objective:** Ensure that all employees understand the importance of AML/CFT controls and their personal responsibility in maintaining compliance.
- **Training Frequency:** Annual mandatory training for all staff, with refresher courses as needed for high-risk areas through the KnowBe4 platform.
- **Core Topics:**
  - Overview of AML/CFT policies and obligations
  - Identifying and reporting suspicious activities
  - The importance of KYC and CDD
  - Preventing money laundering and terrorist financing through employee vigilance
  - Case studies and real-world examples of AML failures and consequences

#### **New Staff Training**

- **Objective:** Educate new employees on the institution's AML/CFT policies, procedures, and controls immediately after recruitment.
- **Training Frequency:** Training must be completed within the first two weeks of employment.
- **Core Topics:**
  - Introduction to AML/CFT obligations and the institution's policies
  - Procedures for customer due diligence, transaction monitoring, and reporting
  - Measures to prevent money laundering and terrorist financing
  - Internal controls and employee responsibilities
  - Ethical conduct and adherence to company policies
  - Case studies and real-world examples of AML failures and consequences

## **14. Review and Update**

The AML Manual is subject to review at least **annually** by the **Anti-Money Laundering Compliance Officer (AMLCO)** and the Board of Directors to ensure its continued effectiveness and alignment with regulatory expectations. In addition to the annual review, the Manual must also be reviewed and updated whenever there are material changes to the business model, operational structure, or when changes in applicable laws, regulations, or regulatory guidance necessitate such revisions. This ensures that the Manual remains current, comprehensive, and fit for purpose in addressing the Company's AML obligations.