

Anti-Money Laundering and Terrorist Financing Policy

Last Updated: 12th September 2024

1. AML Policy Scope and Objectives

OXilium N.V. (the "Company") has zero tolerance for money laundering, terrorist financing, or any other illicit activities and is committed to implementing policies, procedures, and controls based on the highest industry standards and best practices. This policy applies to all employees, Board members, officers, contractors, and consultants of the Company.

This document serves as an overview of the Company's AML compliance regime and procedures, aimed at partners, clients, vendors, contractors, employees, regulators, law enforcement, and other stakeholders. The Company is dedicated to ensuring that all employees actively participate in preventing the misuse of its services for money laundering or terrorist financing.

2. Legal Framework and Compliance

OXilium N.V. operates under the laws of Curaçao with Company Number 165075 and holds license number **OGL/2024/1601/0909** issued by the Curaçao Gaming Control Board under the **National Ordinance on Offshore Games of Hazard (NOOGH)**.

The Company's AML program is designed to be compliant with applicable legislation, regulations, and directives, which include but are not limited to the following:

- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering.
- EU Regulation 2015/847 on information accompanying transfers of funds.
- L188(I)2007 - Prevention and Suppression of Money Laundering Activities Law as amended up to March 17th, 2021.
- Various EU Regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods.
- European Business Law of 18 September 2017 on the prevention of money laundering and limitation of the use of cash.
- FATF Recommendations for International Standards on combating Money Laundering and the financing of terrorism and proliferation (AML/CFT).
- The **National Ordinance on Offshore Games of Hazard (NOOGH)**.

2. Money Laundering

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source can be considered money laundering (ML). It is the process of making dirty money look clean.

Money laundering consists of three phases:

Placement: Introducing illegal proceeds into the financial system through financial institutions, casinos, shops, and other cash-intensive businesses. This includes buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks, and cryptocurrency, and then requesting pay-outs and inserting funds into gaming machines and immediately claiming those funds as credits.

Layering: Converting the proceeds of crime into another form to disguise the audit trail, source, and ownership of funds. This can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring, refining, and gambling accounts held for storing money and hiding them from the authorities.

Integration: The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples include the purchase of luxury assets, financial investments, and investing in gaming companies or commercial investments.

3. Financing Terrorism

Financing of Terrorism is the financing of terrorist acts, terrorists, and terrorist organizations. A terrorist act is an act intended to intimidate a population or compel a government or an international organization to do or to abstain from doing any act.

The most basic difference between the financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, terrorists use methods similar to those used by criminal organizations to launder money, such as cash smuggling, structuring, wire transfers, purchase of monetary instruments, and the use of debit and credit cards.

While money laundering is concerned with obscuring the source of funds, financing terrorism is mostly concerned with obscuring the end recipient of the funds.

4. Distribution of the AML Policy

This AML Policy has been drafted by the Compliance Officer and has been reviewed and approved by the Executive Management Team. The Policy will be distributed to all staff (frontline, leads, managers, and owners) and will be redistributed when updated.

The Compliance Officer is responsible for providing a report to the Executive Management team for review once every twelve (12) months to determine the effectiveness of the Policy and related operational procedures, and shall provide recommendations to management as to proposed operational or policy enhancements.

The Executive Management team shall review the content of this Policy for necessary updates not less frequently than once every twelve (12) months.

Recommendations and feedback will be given to the Compliance Officer. With the exception of directives from relevant authorities, any proposed amendments to the Policy require the review and approval of the Compliance Officer, the Executive Management team, and legal counsel.

5. Compliance Officer – Money Laundering Officer

The management board of the Company shall maintain a Compliance Officer who acts as a contact person with regulators and performs AML/CTF duties and obligations of the Company. The Compliance Officer reports directly to the management board and has the competence, means, and access to relevant information across all structural units of the Company.

Only a person who has the education, professional suitability, abilities, personal qualities, experience, and impeccable reputation required for the performance of the duties listed below may be appointed as a Compliance Officer.

Reporting Structure and Independence

The Compliance Officer holds no other position within the organization or any affiliated company or supplier and operates independently from all other functions within the organization to ensure that actual or perceived conflicts of interest do not occur.

Subject to oversight by the Board, the Compliance Officer has the authority to act independently from other functions within the organization to fulfill the roles and responsibilities noted below. The Compliance Officer has the full and public support of the executive management team in executing his duties. All staff are required to assist the Compliance Officer in fulfilling these duties.

Duties and Responsibilities of the Compliance Officer/MLRO

The Money Laundering Reporting Officer (MLRO) or Compliance Officer is responsible for financial regulations and personal data compliance requirements, ensuring the company's AML policy corresponds to the international system. Furthermore, the MLRO is responsible for oversight and management of all compliance-related functions within the Company and its affected suppliers, including the protocols described in this Policy. Compliance Officer/MLRO duties include (but are not limited to) the following:

- Ensure that procedures are in place to ensure compliance with all applicable legislation, regulations, guidelines, codes of practice, and Company policies and procedures.
- Report to the CEO and inform Senior Management of the results of any corrective actions taken.
- Attend regular Compliance Meetings with selected Senior Management, prepare an agenda for them, and take, circulate, and maintain the minutes thereof.
- Update and maintain any compliance-related policies, including this AML Policy.
- Plan and coordinate training activities for all departments to include key regulatory areas, including the significance of regulatory compliance as a whole, ID and age verification, fraud, anti-money laundering, and problem gambling.
- Be the point of contact with the involved Regulator(s).
- Investigate and report any breaches of applicable laws, regulations, guidelines, codes of practice, and Company policies and procedures to Senior Management and, as appropriate, to the Regulator.
- Consult with staff representatives and attend staff meetings on compliance topics.

- Manage regular reviews of the Company's internal control system to ensure that it accurately reflects the current operation of the business and report any discrepancies/oddities to relevant senior management.
- Maintain records of high-risk clients and report suspicious activities, if any.
- Assist with the implementation of the Anti-Money Laundering policy.
- Arrange for inspections from third-party organizations and eliminate mistakes in the program, if any.
- Oversee the relationship and train Company employees to use software effectively to assist with the application of aspects of the AML Policy.

6. Company Policy and Commitment

The Company will ensure it has appropriate policies and procedures in place to complement this AML policy, in compliance with applicable regulations and recommendations from International and European approved organizations, bodies, directives, and monitoring of adherence to those policies.

Staff members will be trained in all relevant AML processes, awareness, and procedures in accordance with the latest regulatory evolutions and will actively participate in preventing the services of the Company from being exploited by criminals for money laundering or terrorist financing purposes.

The objectives of this and related policies are:

- Ensuring the Company is compliant with all applicable laws, statutory instruments of regulation.
- Protecting the Company and its staff as individuals from the risks associated with breaches of the law, sanctions, regulations, and supervisory requirements.
- Preserving and protecting the Company's reputation against the risk of reputational damage presented by implication in money laundering and terrorist financing activities.
- Making a positive contribution to the fight against crime and terrorism.

7. Screening and Monitoring

AML screening is performed to fulfill three main objectives:

- Establishing an accurate risk assessment.
- Avoiding violating sanctions.
- Protecting the company and its stakeholders from regulatory fines.

Account Screening

Account - Name Screening is one of the methods used for risk assessment of existing or potential customers of organizations under the AML obligation.

Upon a customer's account opening process, a preliminary screening, both automated and manual, will be conducted to identify potentially linked or other suspect account activities compared to the customer profile. The main purpose of the Company is to control their existing and potential customers against sanctions, PEP, banned lists, wanted lists, and adverse media data to prevent false

positives and false negatives by classifying their customers according to their risk levels. This protects the Company from regulatory penalties and avoids violating various sanctions.

As risk levels of customers change over time, the Company will regularly check the risk level of their existing customers through screening. The Company will maintain an updated record of customers by performing online verification on them. All AML procedures, policies, and controls are regularly reviewed and updated to ensure that they consider new risks that may arise.

Such screening searches for potentially suspect elements include the following:

- Accounts that may depict similar information.
- Two or more accounts utilizing the same email address upon creation.
- Customers with more than one account.
- Customers who originate from high-risk or sanctioned countries.
- Any other suspicious information/activity identified or suspected by the Fraud or Financial Services teams.

In the event that any of the foregoing screening identifies potential issues, the Financial Services team is notified automatically and will investigate and enforce applicable business and regulatory rules accordingly. Such business rules may result in a variety of potential risk mitigation steps, including closure of the account, escalation to the Fraud Department for enhanced diligence, limitation of deposit or withdrawal methods, imposition of deposit limits, etc.

8. Enhanced Due Diligence (EDD)

In certain cases, some customer relationships and large transactions demonstrate higher AML or fraud risks to the Company. In such instances, and in addition to regular Customer Due Diligence protocols, the Company shall carry out Enhanced Due Diligence (EDD) for further risk investigation.

Risky customers and transactions pose a greater risk and cannot be detected by Customer Due Diligence (CDD) procedures. In these cases, EDD procedures will be applied to create higher identity assurance by taking the customer identity and addressing and evaluating the customer's risk category.

During the enhanced due diligence process, the Company will take additional steps to aid the identification of a potential customer, including (but not limited to) personal and financial background. This may involve obtaining additional evidence to verify the individual in question, facilitated by third-party verification tools. This may also include obtaining evidence to verify particular aspects of the customer's identity and verified confirmation to establish the source of funds of the customer.

The Company's Fraud Department will have access to a variety of tools through suppliers and databases used to verify submitted documentation (e.g., driver's licenses, passports, IDs, proof of residences, etc.).

The circumstances that may trigger additional concern and require Enhanced Due Diligence (EDD) are noted below:

- The customer or potential customer is situated in a country or territory that does not apply to the Company's geographical market.
- The customer or potential customer is situated in a blacklisted country or a country supporting terrorist activities.
- The customer or potential customer is or appears to be a Politically Exposed Person (PEP) or a close spouse or family member (outlined below).
- The customer has carried out transactions that favor anonymity, for example, deposits made using cryptocurrencies.
- Any other circumstances reasonably perceived by the Company to pose a high risk of money laundering or terrorist financing.

Under the above circumstances, different documents may be requested from the customer as well as from third-party sources for Enhanced Due Diligence purposes.

The Company associates solely with trusted and approved Providers and Partners who all have effective AML policies in place to prevent the large majority of suspicious deposits from taking place without proper execution of KYC procedures onto the potential customer.

9. Politically Exposed Person (PEP) Definition and Screening

Politically Exposed Persons (PEPs) (as well as their families and persons known to be close associates, as described below) are required to be subject to enhanced scrutiny by the Company. This is because international standards issued by the Financial Action Task Force (FATF) recognize that a PEP may be in a position to abuse their public office for private gain and may use the financial system to launder the proceeds of this abuse of office.

PEP Definition

A PEP is a natural person who is or has been entrusted with prominent public functions, including:

- Head of State.
- Head of government.
- Minister and deputy or assistant minister.
- A member of parliament or a similar legislative body.
- A member of a governing body of a political party.
- A member of a supreme court.
- A member of a court of auditors or the board of a central bank.
- An ambassador, a chargé d'affaires, and a high-ranking officer in the armed forces.
- A member of an administrative, management, or supervisory body of a State-owned enterprise.
- A director, deputy director, and member of the board or an equivalent function of an international organization.

PEPs do not include middle-ranking or more junior officials.

Family Members and Close Associates

A family member of a PEP means the spouse, or a person considered to be equivalent to a spouse, of a PEP; a child and their spouse, or a person considered to be equivalent to a spouse, of a PEP; or a parent of a PEP.

A person known to be a close associate of a PEP means a natural person who is known to be in close business relations with a PEP.

PEP Screening

If an account is identified as a potential match to a PEP list using screening tools, the account shall be immediately frozen pending escalation and review from the Fraud Department. The Company does not accept PEPs; if an account is flagged as PEP, it will be **suspended**.

Enhanced due diligence measures will be applied, involving not only available customer-submitted information but also checks of existing PEP lists and a range of news sources, including online and traditional media outlets. The Compliance Officer will reach out to the appropriate department and offer their recommendations regarding the account.

10. Sanctions Screening

Dealing with persons against whom international sanctions have been imposed poses a great risk to the Company, its Directors, Officers, and Owners.

The Company will perform sanction screening of its customers using the same matching rules as for PEP screening.

The Company will perform screening, at a minimum, against the following sanctions lists:

- UN Sanctions.
- EU Sanctions.
- Sanctions administered by the Office of Financial Sanctions Implementation (OFSI-UK).
- Sanctions administered by the Office of Foreign Assets Control (OFAC-US).
- Sanctions imposed under the International Sanction Act.

All matches (true hits) will be escalated to a Compliance Officer for further action and processing.

11. Suspicious Activity Monitoring

Where the Company identifies an activity or facts whose characteristics refer to the use of criminal proceeds, terrorist financing, or other criminal offenses, or an attempt thereof, or where the Company suspects or knows that it constitutes money laundering or terrorist financing, or the commission of another criminal offense, a Compliance Officer of the Company must report it to the relevant Financial Crimes Unit immediately, but not later than within two working days (48 hours) after identifying the activity or facts or after developing the suspicion.

The Company and all its employees, officers, and directors are prohibited from informing a person, its beneficial owner, representative, or third party about a report submitted on them to the Financial Crimes Unit, or an intention to submit such a report, as well as about the commencement of criminal proceedings.

12. Reporting

If the Company reasonably suspects that a customer and/or an account might be involved in any form of activity that amounts to or is connected with money laundering, the Company will immediately inform the required and appropriate external authorities.

If the Company believes that there is some degree of suspicion after a transaction has taken place and an internal investigation confirms this, the Company will freeze the account and inform the relevant authorities immediately, disclosing all necessary information in the Company's possession as required by law. The Compliance Officer or an authorized staff member will report the activity through the appropriate AML reporting form and submit it to the Regulator or any other competent authority.

Additional reporting procedures are put in place to mitigate the Company's exposure to various forms of money laundering and sanctions. These consist of in-house and third-party reporting/monitoring tools that run daily and weekly. Furthermore, AML reporting procedures such as Suspicious Activity Reports (SARs) and Significant Transaction Reports (STRs) will be conducted and submitted when necessary to the Regulators and also to the appropriate law enforcement authorities if required.

13. Ongoing Training and Development

The Compliance Officer shall ensure that the Company's employees are fully aware of their legal obligations under the AML/CTF regime by introducing a comprehensive employees' education and training program.

The timing and content of the training provided are determined according to the needs of the Company. The frequency of the training can vary depending on amendments to legal and/or regulatory requirements, employees' duties, and any other changes in the business model. The training program aims to educate the Company's employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

The Compliance Officer/MLRO will supply the appropriate AML training (which may consist of in-class, video conference, literature, and seminars) to provide the involved staff with updates on the guidelines and direction on:

- The process of reporting suspicious activity.
- Risk management practices.
- Identification and verification procedures.
- Suspicious transaction identification and reporting.
- Record keeping.
- The type of activity that should be considered significant and critical in detecting possible money laundering (these may be given in reading materials).
- Distinguishing specific incidences that may require re-assessment of a risk-based approach.

The Company consistently implements monitoring processes with the addition of potentially new and future products and/or services it provides to its customers. Implementations and assessments are put in place (and adjusted if required) to mitigate any possible risk of money laundering or terrorist financing where the use of new products and/or services may be vulnerable to exploitation.

These include, but are not limited to:

- Analysis of transactions over specific periods.
- Analysis of new services/products used by the customer.
- Applying limits to activities on new products/services used by the customer for a given time.
- Requests for justification of noticeable irregular activity from the customer.

14. Account and Identity Verification Requirements

As an identity verification measure, the Company must identify and verify its customers to flag potentially risky users and monitor for suspicious activity. Verification processes are designed to help reduce the risks of illicit activity by identifying customers and verifying that their identity is correct. Doing so allows suspicious characters and potentially high-risk users to be flagged and monitored, or banned.

Identity theft is a significant problem in online gambling. Users can fraudulently obtain credit card details and use these payment methods to enter games using someone else's funds. Similarly, users can submit fraudulent documents, playing under other people's identities to avoid the repercussions of terrible losses. One of the most damaging forms of fraud for online gambling is multiple account fraud, where users create fake accounts to play and violate the Company's bonus policy.

The procedure forms must be an integral mechanism for protecting the Company from malicious actors and financial crime, as well as ensuring that the Company is complying with AML regulations.

In order to effectively counter the abovementioned issues, the Company has implemented an Identity and Account Verification process for all users/customers to ensure and confirm that the details of the users and customers registered are accurate and correspond to the particular individual. This process also helps ensure that payment details and methods used are not stolen or used by someone else, creating the general framework for the fight against money laundering and financing terrorism.

Verification Process

Upon the creation of a new account, every customer will need to enter their personal details, including:

- Name and surname.
- Email address.
- Date of birth.
- Country of residence.
- Confirmation of acceptance of the Terms and Conditions of the Company's site(s) and that access to minors under the age of 18 is prohibited.

When the account is created and full identity verification is performed, the following details need to be provided by each customer:

- Full name as it appears on the passport (photo and cover page), driver's license, or national ID card.
- Nationality as it appears on the passport or national ID card.
- Gender.
- Date of birth.
- Full address - recent utility bill, bank statement, or council tax bill.

- Contact details.
- Payment method:
 - Credit Cards: Pictures of the front and back sides of the credit/debit card(s). Only the first six and last four digits of the card number should be visible, with the remaining digits and CVV/CVC code on the back covered. If the card has a signature field, it needs to be signed.
 - Ewallets: Proof of ownership of the wallet.
 - Crypto: Proof of ownership of the wallet and its respective currencies used to fund the account.

Full account verification/re-verification will also be required in the following circumstances:

- If there is a request from a player for a change of account details.
- If the address of a user's first deposit method does not match the address used when registering the account.
- If there is a change in the pattern of deposits or withdrawals or there is a pending withdrawal.
- When a user engages in financial transactions equal to or above the nominated threshold, which is set to 4,000 ANG, 2,000 EUR or any currency equivalent. This can be either one deposit, one withdrawal, or cumulatively.
- When a user engages in occasional financial transactions above the monetary equivalent of 4,000 ANG, 2,000 EUR.
- When a name matches or is similar to that of someone with a history of criminal activity or a PEP.
- When a name matches or is similar to that of someone with a suspected duplicate account.

Furthermore, when a user deposits or requests to withdraw €2,000 (two thousand Euros) or more, the user will be requested to provide supportive evidence of their source of wealth (SOW). Examples of SOW include, but are not limited to:

- Employment history.
- Payslips.
- Tax declaration.
- Bank statements.
- Inheritance funds.
- Investments or profits from business operations.

It is critical that the origin and legitimacy of that wealth are clearly understood. If an employee of the Company cannot determine the legitimacy of the wealth, additional evidence and/or information may be requested. An email will be sent to customers guiding them through the procedure and requesting additional evidence.

Performing account verifications can sometimes be a timely process and can vary according to individual circumstances.

15. Risk Assessment

The Company has established a Customer Acceptance Policy to perform an accurate and complete risk assessment when accepting customers. The Policy aims to effectively monitor the Company's customers and to enhance compliance of the Company with the policies and regulatory requirements pertaining to the Client Acceptance Policy.

In order to deal with different risks and different regions, the Company will categorize every nation into three different regions of risk.

Region One: Low Risk

For every nation and region, the Account - ID verification process will be required as described in section 14 above.

Region Two: Medium Risk

For every nation from Region Two, the ID - Account verification will be required at a lower deposit and/or withdrawal amount. Specifically, the ID - Account verification process will be triggered after depositing or withdrawing €1,000 (one thousand Euros). For any deposit and/or withdrawal of €2,000 (two thousand Euros), the user will be requested to declare and submit evidence of the source of wealth (SOW).

Users from a low-risk region who change/deposit cryptocurrency(ies) in any other fiat currency will be treated like users/customers from a medium-risk region.

Region Three: High Risk

Regions of high risk are banned, and users will not be allowed to deposit funds. High-risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

Enterprise-Wide Risk Assessment

As part of its risk-based approach, the Company has conducted an AML "Enterprise-Wide Risk Assessment" (EWRA) to identify and understand related risks specific to the Company. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines, such as the services the websites offer. The users to whom services are offered, transactions performed by these users, delivery channels used by the bank, the geographic locations of the bank's operations, customers, transactions, and other qualitative and emerging risks.

The identification of AML risk categories is based on the Company's understanding of regulatory requirements, regulatory expectations, and industry guidance. Additional safety measures are taken to address the additional risks the internet brings. The EWRA is reassessed yearly.

16. Money Laundering Risk Assessment

The crucial purpose of the Money Laundering Risk Assessment is to identify the general and specific money laundering risks that the Company is facing, determining how these risks are mitigated by the Company's AML program controls, and establishing the residual risk.

As a result, the Company aims to:

- Identify gaps or opportunities for improvement in its AML policies, procedures, and processes.
- Align the AML compliance program with its risk profile.
- Develop risk mitigation strategies, including applicable internal controls, to lower its business line residual risk exposure.
- Raise awareness of the key risks, control gaps, and remediation efforts.
- Assist senior management with strategic decisions in relation to commercial exits and disposals.
- Ensure that resources and priorities are aligned with its risks.

17. Know Your Customer (KYC)

Formal identification of users and customers upon registration and entry into commercial relations is a mandatory requirement for increasing security and protection against fraud.

The Company requires this procedure as it forms part and parcel of gambling responsibly, along with fraud and financial crime prevention, and is required by the applicable legislation.

Upon the registration of a new account, the Company will check that users are over 18 years of age and verify the identification details of those users (a process called Know Your Customer 'KYC').

Identification Procedure

A copy of the user's passport, ID card, or driving license, each shown alongside a handwritten note mentioning six randomly generated numbers, is required. Also, a second picture with the face of the user/customer is required to ensure validity. The user/customer may blur out all information except for the date of birth, nationality, gender, first name, second name, and picture to secure their privacy. All four corners of the ID and/or passport must be visible in the same image, and all details must be clearly readable, except for the aforementioned details. We might ask for all details if necessary.

An employee may also carry out additional checks if necessary, based on the circumstances.

Proof of Address

Verification of proof of address will be done via electronic checks for which we use a variety of databases. Each customer must provide a recent utility bill (mobile bills excluded), bank statement, or tax bill **issued within the last three months**, or an official document issued by the government that verifies the permanent residence of the user.

To make the approval process efficient, please ensure the document sent/uploaded is of clear resolution, preferably in **PDF format**, with all four corners of the document visible, and all text readable.

An employee may conduct additional checks if necessary, based on the situation.

18. Management of Compliance and AML Policies

It is the Company's policy to monitor its compliance program with legal and regulatory AML/CFT requirements. The Policy will be reviewed annually, and amendments added accordingly when new products or regulations are introduced.

The effectiveness of the Company's AML/CFT program is regularly evaluated to ensure it remains current and is aligned with business activities, regulatory developments, industry standards, and best practices. By doing so, the Company adheres to all applicable laws and regulatory requirements in the jurisdictions in which it operates.

19. Data Retention

The Company must retain the documents and information which served for identification and verification of clients, including data processed through third-party verification services, for no less than five years after the termination of the business relationship, unless otherwise required by law.

The Company is allowed to process personal data gathered upon registration of an account with our Company only for the purpose of preventing money laundering and terrorist financing, and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

20. Cooperation and Exchange of Information

The Company cooperates with supervisory and law enforcement authorities in preventing money laundering and terrorist financing, thereby communicating information available to the Company and replying to queries within a reasonable time, following the duties, obligations, and restrictions arising from legislation.

For any general inquiries regarding our policies, or if you have a problem or complaint, you can contact our support team at compliance@bahisbey.com with an accurate description to speed up resolution.