

# **Anti-Money Laundering and Counter-Terrorism Financing Policy**

INNOVEX B.V.

Curaçao, 2025

**Document revision history**

| <b>Revision</b> | <b>Date</b> | <b>Purpose</b>             | <b>Approver</b>               | <b>Security</b> |
|-----------------|-------------|----------------------------|-------------------------------|-----------------|
| v 1.1           | 07.04.2025  | For internal service needs | Claire Godschalk)<br>Director | Confidential    |

**Contents**

|                                                                      |    |
|----------------------------------------------------------------------|----|
| 1. THE POLICY .....                                                  | 3  |
| 2. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING .....      | 3  |
| 3. APPLICABILITY AND REGULATORY FRAMEWORK .....                      | 4  |
| 4. THE COMPANY'S OBLIGATIONS .....                                   | 4  |
| 5. SCREENING & BUSINESS RISK ASSESSMENT .....                        | 6  |
| 5.1. CUSTOMER RISKS .....                                            | 7  |
| 5.2. CUSTOMER ACCEPTANCE POLICY.....                                 | 7  |
| 5.3. DUE DILIGENCE.....                                              | 7  |
| 5.4. ONGOING DUE DILIGENCE .....                                     | 8  |
| 5.5. ENHANCED DUE DILIGENCE .....                                    | 9  |
| 5.6. IDENTIFICATION.....                                             | 10 |
| 6. REPORTING OF SUSPICIOUS MONETARY OPERATIONS OR TRANSACTIONS ..... | 10 |
| 7. DATA STORAGE .....                                                | 12 |
| 8. EMPLOYEE DUE DILIGENCE.....                                       | 12 |
| 9. TRAINING .....                                                    | 13 |
| 10. INTERNATIONAL SANCTIONS .....                                    | 14 |
| 11. OFFENCES AND SANCTIONS .....                                     | 15 |
| 12. APPENDIX A.....                                                  | 16 |
| 13. APPENDIX B .....                                                 | 17 |
| 14. APPENDIX C.....                                                  | 18 |

## 1. THE POLICY

The Policy on Anti-Money Laundering and Counter-Terrorism Financing (hereinafter – “the Policy”) outlines the general unified standards and procedures of anti-money laundering and combating terrorism financing which must be adhered to by INNOVEX B.V., (“the Company”) its directors, officers and employees.

In any country or jurisdiction where the applicable anti-money laundering and counter-terrorism financing laws and regulations require INNOVEX B.V. to establish higher standards, such country standards must be adhered to.

Compliance with this Policy is mandatory and essential for ensuring that INNOVEX B.V. is fully compliant with applicable anti-money laundering and counter-terrorism financing laws and regulations of respective countries and jurisdictions.

INNOVEX B.V. is committed to an annual review and critical reassessment of this Policy considering the Company's business strategies, goals and objectives on an ongoing basis.

INNOVEX B.V. will always seek to disrupt this activity by cooperating fully with the authorities and reporting all suspicious activity to the Financial Intelligence Unit.

## 2. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the “layering” stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Broadly, the international anti-money laundering provisions are aimed at requiring to:

- Identify Customers and suspicious transactions at the placement and layering stages.
- Keep adequate records which should prevent the integration stage being reached and provide an audit trail for investigators.
- Report suspicious activity or behavior to the relevant regulatory or legislative authority.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

### 3. APPLICABILITY AND REGULATORY FRAMEWORK

The Company is bound by the Government of the Country of Curaçao with regards to Anti-Money Laundering and Countering Financing of Terrorism (hereinafter – “**AML - CFT**”). The local authorities in charge of the supervision of AML - CFT matters for the gaming sector are the Curaçao Gaming Control Board (GCB) (<https://www.gamingcontrolCuraçao.org>) and the local Financial Intelligence Unit (“FIU”).

The Curaçao online gaming industry is licensed and regulated under the National Ordinance on Games of Chance NOGC (Landsverordening op de kansspelen, PB 2024, no. 157, “LOK”) and the FIU Curaçao which is the authority supervising adequate reporting of unusual transactions (<http://www.mot.cw/>).

The following laws and regulations are applicable to the Company for the reporting of unusual transactions in Curaçao:

- The National Ordinance on Games of Chance NOGC (Landsverordening op de kansspelen, PB 2024, no. 157, “LOK”)
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (2025)
- National Ordinance Identification when rendering Services (NOIS) (PB 2017, nr 92)
- National Ordinance Reporting Unusual Transactions (NORUT) (PB 2017, nr 99)
- Indicators for detecting and reporting Unusual Transactions (PB 2015, nr 73)
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63)
- National Ordinance of Money Laundering (1993)
- National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002

The Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering (“FATF”) and the Guidelines and instructions of the European Commission as well as all six Directives of the European Union on AML and CFT.

The AML/CTF Policy applies to INNOVEX B.V. and shall be communicated with all employees of the Company, as well as the subsidiaries and affiliated companies within the group to which INNOVEX B.V. outsources some of its operations, to ensure they are aware of their responsibilities under AML/CTF regulations and the policies set out by the Company. For each version update, the Policy shall be communicated to its Employees and other Staff. The policy shall also be shared with any third party entering into a contract with the Company who has any access to transactional Customer data or information which might otherwise present Money Laundering and/or Terrorism Financing (hereinafter – “ML/TF”) risks.

### 4. THE COMPANY’S OBLIGATIONS

The measures, procedures and controls defined in this Policy are kept under regular review so that risks resulting from changes in the characteristics of existing clients, new clients and services are managed and countered effectively. The Policy is periodically (at least once a year) updated by the MLCO based on the general principles set up by the Company’s Director in relation to the prevention of Money Laundering and Terrorist Financing.

INNOVEX B.V. must designate an MLCO who will be responsible for organizing the implementation of money laundering and/or terrorist financing prevention measures as specified in the Money Laundering Regulation and for liaising with the Financial Intelligence Unit Curaçao (FIU) Curaçao.

- Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a MLCO.

The MLCO obligations include but are not limited to:

Establishment of appropriate internal control procedures with the purpose of prevention of monetary operations and transactions related to money laundering and/or terrorist financing: Customer and beneficial owner due diligence, submission of reports and information to the Financial Intelligence Unit Curaçao, storage of information according to Money Laundering Regulation, risk assessment, risk management (taking into account the type of product, service or transaction, geographical risk, etc.), compliance management and communication;

- Undertaking of appropriate measures so that their relevant employees and/or subcontractors are aware at all times of the provisions currently in force. Such measures shall include participation of the relevant employees and/or subcontractors in special ongoing training programs to help them recognize operations which may be related to money laundering and/or terrorist financing and provision of instruction to said employees as to how to proceed in such cases.
- Controlling overall compliance policy for prevention of money laundering and/or terrorist financing and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems.
- Keeping copies of all training materials. Updated AML training is given annually at minimum plus additional training when the need arises, for example in the case of significant changes in the Legislation. Records must be retained of all training sessions including dates, personnel, who received training (name, surname, functions in the Company, their signatures), compliance officer who trained staff (name, surname, functions in the Company, their signatures).
- Monitoring all amendments in the Legislation aimed at prevention of money laundering and/or terrorist financing and updating internal instructions according to up-to-date information. The internal instructions must be updated at least once a year.

All INNOVEX B.V. employees and/or subcontractors are responsible for considering the Policy and understanding responsibilities. All staff members must ensure that INNOVEX B.V. procedures are adhered to and must obtain all documentary evidence as outlined within the Policy. In addition, employees and/or subcontractors must ensure that all suspicious circumstances are immediately reported to MLCO.

A dedicated 'Suspicious Transactions' email box has been created which is available to all employees and/or subcontractors ([compliance@innovexbv.com](mailto:compliance@innovexbv.com)). This mailbox is to be used for all employees and/or subcontractors to report accounts they suspect of money laundering and/or terrorist financing, especially in the cases if behavioral triggers occur. All such suspicious transactions shall be reported internally to the MLCO.

Main ML/TF prevention principles:

- The Company shall only carry on business with persons whom they have adequately identified and in whom there is no suspicion of criminal or terrorist activity.
- The Company shall undertake all measures at its capacity to not be used as a facility for laundering money or assisting others to do so intentionally or otherwise.
- The Company endeavors to verify the data supplied by the Customers upon registration and first withdrawal request, through methods and data available depending on country of residence.
- The Company must obtain reasonable information, adequately documented and corroborated, about the identity of all the Customers when required to do so under the remote gaming regulations.
- The Company shall take all measures necessary to detect and prevent fraudulent customers and activity through regular monitoring of Customer activity.
- The Company must not impede, by action or inaction, any official investigation of money laundering.
- The MLCO must investigate, analyze, consult and, if appropriate, report the activity to the Financial Intelligence Unit Curaçao and take any other action considered legal and necessary.
- The Company shall, as much as possible, follow the relevant 40 + 9 recommendations of the Financial Actions Task Force ([www.fatf-gafi.org](http://www.fatf-gafi.org)).

- The Company shall follow all the laws and regulations relating to anti-money laundering and prevention of terrorism.
- The Company shall provide the necessary training for its employees in anti-money laundering, prevention of terrorism financing and fraud procedures.
- The Company shall keep records of all procedures carried out and reporting effected.

## 5. SCREENING & BUSINESS RISK ASSESSMENT

For the purpose of identification, assessment and analysis of money laundering and terrorist financing risks related to Principal activity, INNOVEX B.V. conducts risk assessment in accordance with “Business Risk Assessment Guideline”. The steps taken to identify, assess and analyze risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of INNOVEX B.V.

As a result of the risk assessment, INNOVEX B.V. maintains the following risk classification:

- Low risk. Customers who are classified as Low risk are subjected to Standard Due Diligence procedures related to the request for Know-Your-Customer (hereinafter – “KYC”) documentation and constant monitoring of activities on the account.
- Medium risk. If the customer fails to provide the requested documentation at a stage where this is required (i.e. when it has been requested due to defined triggers, like change in risk profile from low to medium/high, turns to become a PEP, starts requesting high volume transactions etc.), the account will be under increased monitoring.
- High risk. Customer activity is the determining factor for the classification of a customer as High-risk. Any Customer for which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High-risk, for which an Enhanced Due diligence procedure is applied.
- The Company shall assure “Business Risk Assessment Guideline” is up to date, reviewed and refreshed in the event of material changes to the risk environment.

AML screening is one of the methods used for risk assessment of the Company's existing or potential customers:

- The Company performs the screening of each customer, to identify high-risk clients and Enhanced Due diligence procedure is applied.
- When conducting the screenings, the Company seeks to achieve three main objectives:
  - Make a risk assessment.
  - Avoid violating sanctions.
  - Protection from regulatory fines.
- With AML screening, dedicated employees ensure that existing or potential Customers are not present in any of the sanctions lists, banned or wanted lists, are not classified as PEPs and do not have any adverse media data on file.
- The Company performs AML screening of its customers in the following cases:
  - Upon account opening and withdrawal requests.
  - As risk levels of Customers change over time.
- The Company should regularly, at least once per year, check the risk level of their Customers following their screening.
- To perform AML screening of any Customer, the Company is required to first obtain the full name and date of birth of the Customer.
- Then with the help of internal checks, the name of the person is screened against all sanctions and watch lists, to ensure that they are not listed in any of them.
- With access to global regulatory databases like watch lists, PEPs and sanctions data, these solutions

- increase the reliability of verification processes.
- Hence, these methods not only provide comprehensive risk control for the Company but allow them to fulfill AML obligations effectively.

## 5.1. CUSTOMER RISKS

INNOVEX B.V. does not allow anonymous gambling. Every player is required to register and identify themselves with INNOVEX B.V., by providing their name, date of birth, address, and contact details. Further details of the KYC process are set out in Section 5, “Screening & Business Risk Assessment”. A registered account is only allowed to be operated by the registered individual, and the Company does not allow third-party use of an account. The system is regularly scanned for links between accounts in the registered details.

Politically Exposed Persons (“PEPs”) and sanctioned individuals are not allowed as Customers. All Customers are checked using various methods and if a match is found, the account shall be blocked with immediate effect, to ensure we do not transact with any sanctioned individuals. Adverse media checks are also conducted regularly. Any match detected during these checks, where there is a high likelihood of being a true match, shall be evaluated by the MLCO to consider whether there is reasonable ground to submit a Suspicious Activity / Unusual Transaction report to the FIU.

The Company shall not rely solely on open-source information and shall make regular contact directly with any Customer identified as potentially risky to verify the Customer information provided and obtain further documentation where required.

## 5.2. CUSTOMER ACCEPTANCE POLICY

INNOVEX B.V.’s Customer acceptance policy is based on what is required under law and in line with the Company’s risk appetite and the risk assessment of the business. Certain types of individuals shall not be accepted as Customers, by either being prevented from registering or blocked from using our site:

- Under 18s (or 21 in some jurisdictions).
- PEPs. Politically exposed persons (PEPs) may be subject to pressure and vulnerable to corruption. We do not accept PEPs as Customers and shall block any such individual from registering or playing on our websites.
- Individuals on FATF, UN, EU, UK or OFAC sanctions lists (see **Appendix A & B** for the compiled list of banned/prohibited countries).
- Residents, in countries deemed to be high risk, to measure AML/CTF risk.
- Individuals where we have reason to suspect involvement in ML/TF or other types of criminal activity.
- Self-excluded Customers, excluded from our websites or any national self-exclusion register available within the license conditions.
- Individuals who have submitted documentation or information which we have reasonable grounds to suspect is fake or fraudulent.
- Customers where an increased risk level in the Customer profile for any reason warranted us terminating the Customer relationship.

## 5.3. DUE DILIGENCE

Customers must be identified, and their identity may be verified prior to establishing a business relationship:

- When there are doubts about the veracity or authenticity of the previously obtained identification data of the Customer .
- In any other case, when there are suspicions that the act of money laundering and/or terrorist financing is, has been or will be carried out.
- Before establishing a business relationship with the Customer, INNOVEX B.V. employees and/or subcontractors must apply the following due diligence measures:
  - Identification of a Customer and verification of the submitted information based on information obtained from a reliable and independent sources, including using means of electronic identification and of trust services for electronic transactions.
  - Verification of a Customer's residential address by request for provision of secondary document such as bank statement or utility bill showing residential address.
  - Verification of a Customer's e-mail address by sending a letter with verification link.
- INNOVEX B.V. shall be prohibited from establishing relationships without requesting the Customer to submit data confirming their identity, or where there is a substantiated suspicion that the data recorded in these documents is false or falsified.
- INNOVEX B.V. employees and/or subcontractors shall be prohibited from establishing or continuing relationships and carrying out transactions when it is not possible to fulfil the due diligence requirements established in this Policy:
  - where, in the cases established by this Policy, the Customer fails to submit the data confirming his identity, or where he submits incomplete data.
  - where the data are incorrect, where the Customer avoids submitting the information required for establishing his identity or the submitted data are insufficient for that purpose.

#### 5.4. ONGOING DUE DILIGENCE

INNOVEX B.V. must apply Customer due diligence measures not only in respect of new Customers but also in respect of existing ones, having regard to the level of risk, in the event of new circumstances or new information related to the determination of the level of risk posed by the Customer, their identification information, activities and other relevant circumstances.

Continuous monitoring is in place to track Customer behavior and where transactions are deemed to be unusual, further investigations are undertaken by the Compliance team. These investigations will include, but not be limited to, the following:

- Inactivity period followed by intense activity.
- Game type behavior and amounts played.
- Withdrawals amount against Deposits amounts.
- Transactional behavior.
- Payment method used.

During the period of cooperation with the Customer, INNOVEX B.V. is obliged in all cases:

- To carry out the ongoing monitoring of the Customer's activity, used payment methods, including scrutiny of transactions undertaken throughout the course of such relationships, to ensure that the transactions being conducted are consistent with INNOVEX B.V. knowledge of the Customer, risk profile as well as the source of funds.
- To ensure that the documents, data or information submitted by the Customer during due diligence are appropriate, relevant, regularly reviewed and kept up to date.

- To monitor the achievement of the threshold of €2000 Euro deposited into the Customer's account, whether in a single transaction or in several transactions that make up the specified amount. The Company calculates the Euro two thousand (€2,000) deposit threshold on the basis of a rolling period of one hundred and eighty (180) days.
- INNOVEX B.V. must pay attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and in particular to complex or unusually large transactions, and relationships or deposits/withdrawals with Customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards. INNOVEX B.V. must examine the basis for and purpose of execution of such operations or transactions and the results of the investigation must be recorded in writing.
- INNOVEX B.V. may, in accordance with internal policies and internal control procedures, refuse to execute the deposits/withdrawals and terminate the transactions or relationship with the Customer, where:
  - The Customer avoids submitting, or refuses to submit, additional information to the Company, at its request and within the specified time limits.
  - Where there is suspicions or substantial grounds to suspect that money laundering and/or terrorist financing was, is, or will be performed, or it has been attempted.
  - Where there are suspicions or substantial grounds to suspect that the Customer's funds have been obtained from criminal activity.
  - Where there is suspicions or substantial grounds to suspect that the transactions or activities are related to terrorist financing.

## 5.5. ENHANCED DUE DILIGENCE

Measures of enhanced customer due diligence goes beyond that of the CDD. Enhanced measures are warranted especially in cases identified as high risk. The checks shall cover (but not limited to):

- Suspicious Transactions (see Business Risk Assessment Guideline).
- Customers located in a country that the Financial Action Task Force (FATF) deems sensitive.
- Politically Exposed Persons (PEP's).
- A person performing prominent public functions.
- A close associate of a person performing a prominent public function.
- Clients reached a threshold set in Section 5.4.
- Other Clients that the Company considers to be high-risk in accordance with Business Risk Assessment Guideline.

In the case of High-risk clients, INNOVEX B.V. applies the following additional measures to effectively manage and mitigate its risks:

- Requiring the quality and extent of requisite identification data to be of a certain standard (e.g., documents from independent and reliable sources, certified documents, third person information, documentary evidence).
- Obtaining additional data and information from the Customer, where this is appropriate for the proper and complete understanding of their activities and source of wealth, source of funds.
- Screening against sanctions and government watch lists.
- Assessing the individual's history, reputation, and personal and professional background through review of public records – including civil, criminal and bankruptcy / insolvency records, identification of professional affiliations.
- Search for adverse media and internet research.
- Applying of ongoing monitoring of High-risk Customers' transactions and activities.

The Company shall use all reasonable efforts to obtain this information. All information should be checked against all available databases.

## 5.6. IDENTIFICATION

INNOVEX B.V. identifies the Customer and retains the following data on the person:

- Name, surname.
- Personal identification code or, if not, the date and place of birth and the country of residence.
- Gender, date of birth (age).
- Customer's email address.
- Customer's address and phone number.
- Payment details.

INNOVEX B.V. verifies the correctness of the data specified by the Customer, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified above, or an equivalent document, the person is identified, and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

- Required proof of identity – must include copies of the following:
  - Passport or Driving License or National Identity Card.
  - Proof of Address – Utility Bill / Official or Bank Correspondence.
  - Proof of ownership of the linked payment method – Bank Statement or Card Statement (figures may be blocked out).
  - These documents shall be preferably sent in digital format signed with a person's own digital signature. INNOVEX B.V. may ask for these documents also in notarized format (whereby the validity (originality) of the document is confirmed by the notary public).

In the event behavioral triggers (see the Business Risk Assessment Guideline) occur, INNOVEX B.V. may ask from the Customer presentation of additional documents. In certain situations, it may be necessary to establish the source of funds and the wealth of the Customer, or ask for other information in respect of the nature of the transaction, aim of transaction etc. The Company shall use all reasonable efforts to obtain this information.

## 6. REPORTING OF SUSPICIOUS MONETARY OPERATIONS OR TRANSACTIONS

INNOVEX B.V. must pay attention to any activity which they regard as likely, by its nature, to be related to money laundering and/or terrorist financing, and to complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, and relationships or monetary operations with Customers from third countries in which, based on the information officially published by international intergovernmental organizations, money laundering and/or terrorist financing prevention measures are insufficient or do not correspond to international standards. INNOVEX B.V. must examine the basis for and purpose of execution of such operations or transactions and the results of the investigation must be recorded in writing.

INNOVEX B.V. must report to the Financial Intelligence Unit Curaçao any suspicious or unusual monetary operations or transactions.

Suspicious or unusual monetary operations or transactions, including:

- Cases where it is aware of, obtains information concerning, has suspicions or has substantial grounds to suspect that money laundering and/or terrorist financing was, is, or will be performed, or it has been attempted.
- Cases where they have suspicion or sufficient grounds to suspect that the Customer's funds have been obtained from criminal activity.
- Cases where they have a suspicion or sufficient grounds to suspect that the transactions or activities are related to terrorist financing.

INNOVEX B.V. must report on unusual monetary operations or transactions mentioned in Section 10.3. to the Financial Intelligence Unit Curaçao immediately, but not later than within two working days after identifying the activity or facts or after becoming suspicious.

INNOVEX B.V. must immediately submit to the Financial Intelligence Unit Curaçao all the information available to INNOVEX B.V., which the Financial Intelligence Unit Curaçao requested in its enquiry.

Upon establishing that their Customer is carrying out a suspicious monetary operation or transaction, INNOVEX B.V. must suspend the operation or transaction disregarding the amount of the monetary operation or transaction and, not later than within one working day from the suspension of the monetary operation or transaction, report this operation or transaction to the Financial Intelligence Unit.

Where the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction or professional act shall be carried out or the official service will be provided, and a report will be submitted to the Financial Intelligence Unit:

- A report to the FIU is submitted via GoAML reporting portal (link to register in [GoAML](#) ).
- The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.
- The structural unit of INNOVEX B.V., a member of a management body and any employee are prohibited to inform a person about a report submitted on them to the Financial Intelligence Unit, plan to submit such a report or the occurrence of reporting as well as about any precept made by the Financial Intelligence Unit Curaçao or about the commencement of criminal proceedings. After a precept made by the Financial Intelligence Unit Curaçao has been complied with, INNOVEX B.V. may inform a person that the Financial Intelligence Unit Curaçao has restricted the use of the person's account or that another restriction has been imposed.

The prohibition is not applied upon submission of information to competent supervisory authorities and law enforcement agencies.

The exchange of information must be retained in writing or in a form reproducible in writing for the next five years and information is submitted to the competent supervisory authority at its request.

INNOVEX B.V., its employee, representative and/or the person who acted on its behalf are not liable for damage caused to a person or Customer participating in a transaction made in economic or professional activities, in performing a professional act or in the provision of a professional service:

- upon performance of duties and obligations arising from Anti Money Laundering and Terrorist

Financing Prevention regulations in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit.

- in connection with the performance of the duty to report in good faith.

INNOVEX B.V. establishes a system of measures ensuring that the employees and representatives of the Company who report of a suspicion of money laundering or terrorist financing to the Financial Intelligence Unit Curaçao are protected from being exposed to threats or hostile action by other employees, management body members or Customers of the Company, from adverse or discriminatory employment actions.

## 7. DATA STORAGE

INNOVEX B.V. must keep a register of reports of suspicious monetary operations and transactions specified in Section 6, "Reporting of Suspicious Monetary Operations or Transactions" of this Policy.

INNOVEX B.V. must keep a register of the Customers with whom transactions or relationships were terminated under the circumstances specified in Section 5.5 "Enhanced Due Diligence" of this Policy or under any other circumstances related to violations of the Policy.

Register data shall be stored in electronic form for five years from the date of termination of transactions or relationships with the Customer.

Copies of the identity documents of the Customer, other data received at the time of establishing the identity of the Customer and account and/or agreement documentation (originals and/or copies of the documents) must be stored for five years from the date of termination of transactions or relationships with the Customer.

The correspondence with the Customer must be stored in paper or electronic form for five years from the date of termination of transactions or relationships with the Customer.

The documents confirming a monetary operation or transaction and data or other legally binding documents and data related to the execution of monetary operations or conclusion of transactions must be stored for five years from the date of execution of the monetary operation or conclusion of the transaction.

Records of the results of the investigation specified in this Policy shall be stored for five years in paper or electronic form.

Time limits for storage may be additionally extended upon receipt of a reasonable request from a competent institution.

INNOVEX B.V. must store the personal data of staff referred to in Section 8 "Employee Due Diligence" of this Policy for five years upon termination of employment, unless longer storage is required by applicable Labour laws and regulations in the country of residence of the employee.

## 8. EMPLOYEE DUE DILIGENCE

Employee due diligence is a procedure used to screen employees. The screening procedure aims to identify and minimize business exposure to the risk of money laundering and terrorism financing. For the avoidance of doubt, same procedures apply not only to the contractual employees of the Company, as per Labour laws and regulations, but also to the contactors and/or subcontractors of the Company.

An employee's due diligence is based on the risk assessment of the business and the roles within it.

Any employee whose role means they might be able to facilitate money laundering or terrorism financing must be screened. This includes:

- Prospective employees before they are employed to such a position.
- Existing employees before they are transferred or promoted to such a position.
- To screen both current and potential employees the Company should:
  - identify them.
  - verify their identity
  - confirm their employment history (e.g., through references)
  - decide whether they are suitable for the position and do not pose a risk to the Company.

The Company shall take into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of staff.

Roles with duties that might make the employee a target for collusion with, or coercion by, criminal groups must be subject to a tougher check.

The Company must consider checking whether the employee:

- has a criminal record (e.g., through a police check).
- is or has been subject to any regulatory, court or legal action.
- has used bankruptcy laws to their own advantage.
- has lived in high-risk countries or regions.

## 9. TRAINING

In providing the specified categories of employees with the AML/CTF training, INNOVEX B.V. shall take into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of staff. INNOVEX B.V. shall, within the framework of the training, explain to staff the AML/CTF requirements and provide detailed information on the measures and activities the staff are expected to conduct within the framework of their responsibilities.

INNOVEX B.V. shall develop and document a staff training plan which contains at least the following programs:

- An internal training program for staff, which uses internal training resources (hereinafter referred to as the “internal training”).
- An external training program for staff, which uses external training resources, including participation of foreign experts (a qualified person in the AML/CTF area) (hereinafter referred to as the “external training”).
- A training program for new employees (employees who have just started to perform their duties or changed position at INNOVEX B.V. (hereinafter referred to as the “new staff training”).

INNOVEX B.V. shall ensure that the information on the conducted staff training is saved by documenting the following data:

- Name of the training.
- Personal data of the trained employee.
- Position and structural unit of the trained employee.
- Training venue.
- Head and organizer of the training.

- Time of training.
- Duration of the training.
- Result of knowledge tests and certificate obtained, if any.

INNOVEX B.V. shall update the training programs in line with any modifications in internal and external regulations and supply of training programs in the market (for provision of external training).

INNOVEX B.V. shall, at least once a year, assess compliance and efficiency of the training programs and make any necessary changes thereto.

INNOVEX B.V. shall ensure that, in addition to the internal and external training, any employee may obtain the necessary advice from senior employees involved in the AML/CTF risk management.

INNOVEX B.V. shall conduct an appropriate training program before new staff start to perform their duties.

- In addition to the internal training, INNOVEX B.V. shall ensure extraordinary staff training in AML/CTF issues at least in the following cases:
  - New internal and external regulations governing the AML/CTF have come into force and are applicable to the staff of INNOVEX B.V.
  - New products and/or services have been introduced which cause changes in the AML/CTF risk exposure.
  - During the performance of his/her duties an employee violates the internal and external regulations governing the AML/CTF due to insufficient knowledge.

## 10. INTERNATIONAL SANCTIONS

INNOVEX B.V. shall be prohibited to perform any actions the performance of which is prohibited by the international sanctions implemented in the Curaçao.

Prospecting Customers from countries that pose high ML/TF risks which lie outside of the business risk appetite shall be blocked from registration and/or login. The Compliance department reviews the list of accepted countries on a regular basis, in line with certified and credible sources of information regarding the level of ML/TF risks, corruption, political unrest, and countries subject to sanctions (see Appendix A for the compiled list of banned countries), embargos or similar measures, countries with no or little AML Regulations and monitoring by FATF, or countries providing funding and/or support for terrorism.

INNOVEX B.V. shall be prohibited to accept transactions the execution of which would conflict with international sanctions implemented in the Curaçao. Such transactions concluded after the establishment of the implementation of international sanctions:

- In the manner prescribed by this Law shall be null and void, and invalid.
- The fulfilment of the obligations which appeared prior to the Curaçao establishment of implementation of international sanctions in the Curaçao must be terminated immediately or suspended for the duration of the implementation of international sanctions. It shall be prohibited to assume new obligations the fulfilment of which would conflict with international sanctions implemented in the Curaçao.
- Upon the restriction of availability of accounts to the entities with respect to which international sanctions are implemented, expenses associated with routine holding of such accounts may be deducted from them, and interest as well as payments due under transactions, concluded prior to the commencement of the implementation of international sanctions, may be added only if any deductions or additions shall not be

made available to the entity with respect to which financial sanctions are implemented.

## 11.OFFENCES AND SANCTIONS

If the Company does not comply with the compulsory AML/CFT requirements, it is committing an offense, which is an unlawful and punishable act.

The way in which an offence is punished depends on the severity of the offence committed. Offences are subdivided into misdemeanors and felonies.

Felony refers to a serious offence committed for which the lawbreaker will be tried, judged and sentenced by a court in Curaçao and Sint Maarten.

The penalty amount or fine for the various offences is specified in the National Ordinance Reporting Unusual Transactions (NORUT) (PB 2017, nr 99) and the National Decree Penalties and Fines Service Providers (ND PFSP) (NG 2010, no. 70).

The Central Bank will report an offence to be criminally investigated or prosecuted by the law enforcement in circumstances where the offender emphatically refuses to comply with the NORUT and/or NOIS.

Before proceeding to imposing a fine, the Central Bank shall inform the (financial) institution or individual in writing of its intention to impose a fine, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term.

## 12. APPENDIX A

Below is the compiled list of countries/jurisdictions that present AML/CTF strategic deficiencies; however, it is not exhaustive and might also include other countries/jurisdictions that may be subject to restrictive measures (e.g., change in the FATF's Increased Monitoring / Call for Action Lists, and/or countries/jurisdictions with other AML / CFT shortcomings etc.).

- Barbados
- Burkina Faso
- Cambodia
- Cayman Islands
- Cuba
- Ethiopia
- Mali
- Morocco
- Mozambique
- Myanmar
- Nicaragua
- Nigeria
- Fiji
- Pakistan
- Panama
- Senegal
- South Sudan
- Syria
- Trinidad and Tobago
- Uganda
- Yemen
- Iran (black-listed)
- North Korea - Democratic People's Republic of Korea (black-listed)

\* Contested territories that are not internationally recognized:

- Eastern Ukraine
- Transdniestria
- The Crimea Region (Ukraine)
- Abkhazia
- South Ossetia

## 13. APPENDIX B

Below is the compiled list of countries/jurisdictions that are subject to limitations of the applicability of INNOVEX B.V.'s license; however, it is not exhaustive and might also include other countries/jurisdictions that fall under these markets and/or license applicability restrictions.

- |                                    |                                  |
|------------------------------------|----------------------------------|
| • Afghanistan                      | • Belize                         |
| • American Samoa                   | • Belgium                        |
| • Aruba                            | • Bonaire                        |
| • Australia                        | • Bosnia and Herzegovina         |
| • Botswana                         | • Martinique (FR)                |
| • Bonaire                          | • Netherlands                    |
| • Burma                            | • Occupied Palestinian Territory |
| • Burundi                          | • Poland                         |
| • Central African Republic         | • Puerto Rico                    |
| • Curaçao                          | • Qatar                          |
| • Democratic Republic of the Congo | • Republic of Guinea             |
| • Eritrea                          | • Republic of Guinea-Bissau      |
| • Estonia                          | • Russian Federation             |
| • France                           | • Saba                           |
| • French Guyana                    | • Saint Barthelemy               |
| • Greenland                        | • Saint Martin                   |
| • Guadeloupe                       | • Saint Pierre and Miquelon      |
| • Guam                             | • South Africa                   |
| • Holy See (Vatican City)          | • Somalia                        |
| • Iraq                             | • St. Eustatius                  |
| • ISIL and Al-Qaida                | • Sudan                          |
| • Ivory Coast                      | • USA                            |
| • Lebanon                          | • US Minor Outlying Islands      |
| • Libya                            | • US Virgin Islands              |
| • Lithuania                        | • Venezuela                      |
| • Marshall Islands                 | • Zimbabwe                       |

## 14. APPENDIX C

## Player Risk Matrix

| Risk Rating       | Nature                                                                                                                                                                                     | Location                                                                                                                                                                        | Source of funds/Wealth                                                                                                                                                                                                                  | Transaction Size                                                                                                                                 |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Prohibited</b> | Sanctioned individual and PEPs.<br><br>A Customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements | Closed jurisdictions<br><br>A Customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements | Cash<br><br>A Customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements.<br><br>Funds appear to be generated or linked to the proceeds of crime | A Customer that has breached any of the below thresholds but does not comply with the Company's CDD/EDD requirements.                            |
| <b>High</b>       | Professional Gambler<br><br>Customers that are sporting professional betting on sports<br><br>High net worth individuals                                                                   | Named on FATF's Blacklist<br><br>Countries with AML/CFT strategic deficiencies                                                                                                  | Use of over 5 different payments methods                                                                                                                                                                                                | Deposit or withdrawal of EUR 10,000 in any period                                                                                                |
| <b>Medium</b>     | Public profile raises some form of concern e.g., adverse media, social media activity                                                                                                      | Named on FATF's List B.<br><br>Countries which in the opinion of the MLCO represents heightened risk                                                                            |                                                                                                                                                                                                                                         | Deposit or withdrawal or over EUR 3,000 (or currency equivalent) or aggregate in excess of EUR 3,000 (or currency equivalent) in a 30-day period |
| <b>Low</b>        | Individual                                                                                                                                                                                 | Fully compliant with FATF<br><br>No AML/CFT concerns                                                                                                                            | Bank transfer<br>Debit or credit card<br><br>Approved payment service provider                                                                                                                                                          | Under any of the qualifying payment thresholds                                                                                                   |