

Know Your Customer Policy

WILLX N.V.

Last update: October 20, 2025

Introduction This onboarding policy is designed to ensure a secure, compliant, and seamless user registration and verification process for our online gambling platform. It outlines the steps to onboard new users while minimizing risks related to fraud, identity theft, and regulatory non-compliance. This document also includes our Risk and Fraud Prevention Policy, detailing mechanisms like BIN Blocks, velocity checks, transaction amount limits, and advanced risk mitigation strategies.

1. User Registration Process

1.1 Account Creation

1. Users must provide the following details during registration:
 - Full name
 - Date of birth (to verify age compliance)
 - Email address
 - Mobile phone number
 - Residential address
2. Users must create a unique username and a strong password.
3. Users must accept the platform's Terms and Conditions, Privacy Policy, and Responsible Gambling Policy.

1.2 KYC (Know Your Customer) Verification

1. Users must upload the following documents for identity verification:
 - Government-issued photo ID (e.g., passport, driver's license)
 - Proof of address (e.g., utility bill, bank statement, not older than three months)
 - Selfie
2. KYC documents are reviewed in the following statuses:
 - **PASS:** All required documents are approved, enabling full account functionality.
 - **OPEN:** Missing or invalid documents restrict withdrawals but allow deposits and gameplay.

- **FAILED:** Rejected documents restrict withdrawals until valid replacements are submitted.
- 3. The platform employed automated tools to validate document authenticity and match the submitted information with the user's profile.
- 4. Enhanced due diligence (EDD) will be required for high-risk users or users from flagged regions, including verifying the source of funds and monitoring unusual transactions.
- 5. Special cases, such as underage accounts, will result in account closure, balance adjustment, and blacklisting. Refunds will be limited to deposits, excluding winnings.
- 6. Users flagged for discrepancies in personal information (e.g., name, DOB, address) must provide explanations or additional verification, such as a selfie with their ID. If the explanation or the documents are not satisfactory, the account will be closed and blacklisted (if any funds are present on the account, they will be voided for false information provided).

2. Risk and Fraud Prevention Policy

2.1 BIN Blocks

1. The platform maintains a list of restricted BINs (Bank Identification Numbers) associated with high-risk or fraudulent activities.
2. Transactions originating from blocked BINs will be automatically declined.
3. BIN lists will be updated regularly using data from payment processors, industry reports, and fraud intelligence platforms.
4. Real-time monitoring will ensure transactions from new or unlisted BINs are evaluated for risk by our fraud detection systems.

2.2 Velocity Checks

1. Velocity checks will monitor and limit the frequency and volume of transactions:
 - Maximum number of transactions per user in a 24-hour period.
 - Maximum number of attempts per payment method within a specified time frame.
 - Cumulative transaction amounts exceeding preset thresholds within a defined period.
2. Users exceeding these limits will have their transactions flagged and accounts temporarily suspended for review.
3. Historical velocity patterns will be analyzed to refine thresholds and detect emerging fraud trends.

2.3 Transaction Amount Limits

1. The platform enforces minimum and maximum deposit and withdrawal limits:

- Minimum deposit: \$10

VIP Level Daily Limit Weekly Limit Monthly Limit

Standard	\$600	\$3,000	\$12,000
VIP Level 1	\$700	\$3,500	\$14,000
VIP Level 2	\$1,000	\$5,000	\$20,000
VIP Level 3	\$2,000	\$10,000	\$40,000

2. Transactions exceeding these thresholds will require additional verification, such as:
 - Proof of source of funds (e.g., bank statements, payslips)
 - Enhanced due diligence (EDD) review, including a review of the user's transaction history and risk profile.
3. Alerts will notify the risk management team of unusual transaction patterns, such as repeated maximum-limit deposits or withdrawals.

2.4 IP and Geo-Location Monitoring

1. Users attempting to access the platform from restricted jurisdictions will be automatically blocked.
2. Multiple accounts accessed from the same IP address will trigger a fraud alert for further investigation.
3. Geo-location data will be cross-referenced with user-provided information to identify potential discrepancies or use of VPNs/proxies.

2.5 Suspicious Activity Monitoring

1. The platform uses tools to detect unusual activity, such as:
 - Multiple deposits and withdrawals in a short period of time
 - Multiple failed login attempts
 - High-risk geographical locations
 - Sudden changes in user behavior, such as a shift in betting patterns or stakes.
 - Declined deposits for lost/stolen/fraud suspected reasons.
2. Detected anomalies will result in account suspension and manual review.

3. Escalation protocols will involve collaboration with law enforcement or regulatory authorities for high-risk cases.

2.6 Blacklist and Watchlist Management

1. Accounts identified as fraudulent or involved in chargebacks will be added to an internal blacklist.
2. The platform will integrate with external watchlists for known fraudsters and high-risk entities.
3. Blacklisted accounts will be permanently banned, and associated payment methods or devices will also be flagged.

2.7 Behavioral Analytics and Risk Scoring

1. The platform employs behavioral analytics to monitor user activity patterns and assign risk scores to each account.
2. High-risk scores will trigger additional verification steps or account suspension.

2.8 Manual and Continuous Monitoring

1. Continuous monitoring includes adverse media screening, sanctions checks, and device fingerprinting.
2. Manual verification will address document discrepancies, flagged accounts, and suspicious behaviors.
3. Accounts flagged for forged documents or mismatched details will be reviewed and resolved according to predefined escalation protocols. The procedure for handling forged documents in KYC verification involves detecting signs of tampering, flagging suspicious accounts for review, and notifying relevant teams for further investigation. Based on the findings, accounts are either suspended with formal notification and blacklisting for confirmed forgeries or reinstated with notification upon successful validation of resubmitted documents.

2.9 Player Accounts - Suspension and Closure

1. **Customer Risk Assessment**, based on Continuous Monitoring (ongoing monitoring), where the customer's activities are continuously monitored for any changes or updates that could affect their risk profile. The specific monitoring may involve automated or manual systems for transaction monitoring, as well as periodic reviews of customer information and behavior. This also will include trigger events (from the Risk Categorization) and risk factors. Once the risk assessment is revised and updated, appropriate actions are taken based on the customer's new risk level. This could involve adjusting the level of due diligence, implementing additional monitoring measures, or may include terminating the customer business relationship if the risk is deemed unacceptable.

2. **ON-GOING CUSTOMER DUE DILLIGENCE:** An examination of customer's transactions and existing records are to be conducted regularly and updated and KYC documents are to be reviewed every 6 months to consider whether additional documents are required, or risk profile has changed.

Specific Indicators:

- Non-PEP becomes PEP
- Change in player transaction pattern i.e. Money laundering flag
- Data becomes outdated i.e. Valid Identity Card
- Change in Transaction pattern

Failure to provide the required documentation will result in:

- The business relationship with the customer being terminated (account closure)
3. Regarding the **Customer Risk Assessment**, this will be carried out in the case of the business relationship not later than thirty (30) days from when the pre-established threshold Naf. 4,000 (2.000 euro) is met.
Moreover, in case where the imposed timeframe of 30 days has elapsed since the threshold of two thousand (EUR 2,000) and the customer did not provide the requested information and documentation, WILLX's is to consider the business relationship termination with the customer.
4. WILLX N.V is establishing, recording, maintaining and operating appropriate procedures and controls which require verification of the identity of the customer using reliable, independent source documents, data or information, and where there is no cooperation from the customer:
- 1) The ongoing customer relationship or transaction will proceed no further;
 - 2) The business relationship should be terminated and
 - 3) A disclosure to be made to relevant authorities if applicable;

3. Due Diligence – Comprehensive Procedure

Procedure's role is to know who the customer is and to build a customer profile of which the customer's identity can be assessed, and any unusual behavior can be identified. If any such behavior is found to lead to a suspicion of ML/FT, it shall be reported to the FIU.

CDD shall have four measures:

- Identification and Verification of the Customer.
- Identification and Verification of the Beneficial Owner.
- Obtaining Information on the Purpose and Intended Nature of the Business Relationship.
- On-Going Monitoring.

Depending on risk, the Customer Due Diligence shall be simple or enhanced.

3.1 Customer Due Diligence Documents

At registration stage:

- A valid and unexpired national government-issued identity card;
- A valid unexpired passport;
- A valid unexpired residence card;
- A valid unexpired driving licence;

At verification stage:

- A bank statement or reference letter issued by a recognized credit institution or entity carrying out relevant financial business;
- A utility bill (electricity, water bill, internet), mobile phone bills are not accepted;
- Any other government-issued document not mentioned above;

The documents listed above must not be more than three (3) months old.

The documents subjected to verification shall be obtained in hard copies and may be gathered also in

electronic means through, amongst others, electronic mail and audio-visual means. Nonetheless, it is

imperative that such documents shall be clear, legible and of good quality.

The documentation used for identification and verification purposes must be authentic or reproduced

authentic ones.

3.2 Ongoing clients monitoring

The monitoring shall take place in situations in which a client seeks to form or has formed a business

relationship, and not an occasional transaction. The monitoring shall have several steps.

First one is the Scrutiny of Transactions, which consists in using the information provided by the customer to identify any transactions that are unusual.

At this step, any unusual transaction served as red flag or event trigger which shall require immediately

scrutiny of the relationship to establish if a transaction is suspicious and ought to be reported or

whether there is a legitimate and plausible explanation.

The term unusual used here includes transactions which are unusual by their very nature (as they are

suspicious, illogical, or unreasonable), as well as those which are inconsistent with the client's profile

or are significantly different to what is usually carried out or requested by the client.

Second step is the Periodic Review of the information, data and documents held on the client, which

consists in ensuring that information, documents and data on the client, as well as any assessment, remain up-to-date and relevant. Depending on risk assessment, the periodic review shall be performed as follows:

- Low Every 5 years
- Low to Medium Every 3 years
- Medium Every 2 years
- Medium to High Every 1 year

All records of CDD documents and supporting evidence will be kept for five years.

All customer CDD will start at point of reaching the €2,000 threshold (4.000 NAF), moreover The company will have in place a level of on-going monitoring: the capability to determine the moment in time when the Euro two thousand (€2,000 - 4.000 NAF) threshold is met (given the alerts generated

by PIQ), detection of IP addresses, device location, opening of multiple accounts by the same person

(in which are made manually).

3.3 Timing of Verification:

Identification procedures can be conducted:

- Before withdrawals, deposits above thresholds, or continued gameplay beyond regulatory limits.
- Immediately, if suspicious activity is detected.

Application, Extent and Timing of CDD Measures

CDD measures, provide the need to be applied when carrying out transactions amounting to Euro two thousand (€2,000) - (4.000 NAF), or more, whether carried out within the context of a business relationship or otherwise.

The CDD application when reaching €2,000 (4.000 NAF), threshold it's applied in regard to players which are making the deposits through Credit Card; Debit Card; Instant Banking; Bank transfer; E-wallet; E-voucher.

Even before reaching the €2,000 (4.000 NAF), threshold, the Company have measures in place which allow it to apply a level of on-going monitoring.

Regarding these systems, the Company ensures that:

- It's able to determine the moment in time when the Euro two thousand (€2,000)- (4.000 NAF), threshold is met.
- The player does not avoid the application of CDD measures by ignoring the Euro two thousand (€2000) -(4.000 NAF), threshold.
- It's able to deny the application for the opening of an account by a person who has submitted false details.
- It's able to detect instances which give rise to a suspicion of ML/FT.

CDD Process - Threshold deposit Limit Reached (€2,000) - (4.000 NAF) - euro total deposit-calculated in real time since the establishment regarding the business relationship; or on a daily basis taking into account all deposits/ withdrawals effected by a customer since the establishment of the business relationship / First Withdrawal / High Risk player (PEP/Deposit pattern/ Geo Location / Funding Method). Lifetime deposits are taken into consideration and all deposits made by a customer since the establishment of the business relationship will be calculated daily and will be sent to the relevant Departments.

3.4 Customer Due Diligence Obligations:

In case where Player Deposits Fund €2,000 (4.000 NAF), Deposit Threshold is reached, the Company shall determine if the Customer is a PEP, if it's not a PEP the Company will carry out the Customer Risk Assessment which can be evaluated in three stages:

A. LOW :

- Verification of Personal Details
- On-Going Monitoring to detect unusual activities, to keep information and profile updated, and to ensure relationship remains Low Risk
- Report Suspected Cases of ML/FT

B. MEDIUM :

- Collect additional personal details
- Verify personal details using documents with photograph

- Collect source of wealth information
- On-going monitoring to detect unusual activities, and keep information and profile updated
- Report Suspected Cases of ML/FT

C. HIGH :

- Collect additional personal details
- Verify personal details using documents with photograph
- Collect source of wealth information and documentation
- Enhance on-going monitoring to detect unusual activities, and keep information and profile updated
- Take additional measures to address any other risk identified
- Report Suspected Cases of ML/FT

Depending on the risk emerged from a customer, different levels of customer due diligence (CDD) need to be applied, distinguishing between simplified due diligence (SDD), standard customer due diligence (CDD) and enhanced due diligence (EDD).

The eligibility criteria that The Company takes in consideration for *SDD process/ procedures* is the following:

Low-Risk Customer Profile

- No adverse media, sanctions, or PEP matches.
- Clear identity data with no inconsistencies.
- Residency in a low-risk jurisdiction (regulator-defined).

Low-Risk Transaction Behavior

- Low-value deposits and limited betting activity.
- No unusual patterns, rapid spending, or volatility.
- No use of complex payment methods (e.g., crypto, prepaid cards, third-party wallets) unless permitted and risk-rated.

Players under SDD procedures remain subject to:

- Continuous monitoring of activity
- Manual behavioural alerts
- Periodic reviews of risk exposure
- Immediate escalation to the Compliance/AML officer if concerns arise

3.5 EDD (Enhanced Due Diligence) :

EDD is applicable for players who pose a higher risk. EDD measures are further measures to the CDD measures, which the Company shall apply in order to ensure that the increased risks presented by specific business relationships are efficiently monitored and administered.

EDD will be applied in four (4) different scenarios:

- Non-Face-To-Face (where the Company determines that additional EDD measures are required);
- PEPs;
- Suspicion or any other particular cases presenting higher risk as outlined in the Policy;
- Failure to satisfy either aspect of verification.

Therefore, in addition to the CDD measures set out hereabove, the Company shall apply one or more of the following measures:

- Verification through the use of recognized commercial electronic data providers;
- Establishing the identity of the Player by using additional documentation and information wherein the Player shall provide the Company with additional documentation to confirm the personal details by means of documents listed hereabove. The documents obtained in terms of this particular EDD measure are required to be additional to the documents obtained when carrying out CDD and should have been obtained from other independent sources. The additional documents cannot be the same documents obtained for CDD purposes;
- Verify or certify the documentation supplied using supplementary measures. This measure consists in the certification of the documentation used for the purposes of the verification of identity by a warranted legal professional, certified accountancy professional, a notary, a person undertaking relevant financial business or a person undertaking an activity equivalent to relevant financial business carried out in another jurisdiction. Such certification should be evidenced by a written statement stating that:
 - the document is a true copy of the original document;
 - the document has been seen and verified by the certifier; and
 - the photo is a true likeness of the applicant for business or the beneficial owner

The certifier must sign and date the copy document (indicating his name clearly beneath the signature) and clearly indicate his profession, designation or capacity on it and provide his contact details.

3.6 PEP (Politically Exposed Persons)

PEP as a natural person who is or has been entrusted with prominent public functions and includes his immediate family members or persons known to be close associates of such persons but shall not include middle ranking or more junior officials. For the purposes of the Player acceptance

process, the Company shall apply EDD in relation to PEPs residing in another Member State of the Community or in any other jurisdiction.

The data required to determine if a customer (or its beneficial owner) is a PEP can be obtained either from the customer (e.g. by completing a standardized self-declaration as to his/her status or, to the extent which may be applicable, that of its beneficial owners) or by using reliable electronic databases to screen their customer database. In establishing the source of wealth and source of funds of a PEP, the Company is to determine the extent of the information and/or documentation requested on the basis of the risk posed by the customer.

In a risk-based approach, the frequency of checks for Politically Exposed Persons (PEPs) can vary based on the assessed risk level

High-Risk Customers (including PEPs):

- Initial Due Diligence: At the start of the business relationship.
- Ongoing Monitoring: At least quarterly, or more frequently if there are significant changes in the customer's profile or transactions.
- Regular Re-Screening: Every 6 months to ensure that the customer's status has not changed and that there are no new risk factors.

Medium-Risk Customers:

- Initial Due Diligence: At the start of the business relationship.
- Ongoing Monitoring: Semi-annually, to identify any unusual activities or changes in customer status.
- Regular Re-Screening: Annually, to ensure continued compliance and to identify any new risk factors.

Low-Risk Customers:

- Initial Due Diligence: At the start of the business relationship.
- Ongoing Monitoring: Annually, unless there are specific reasons to conduct more frequent checks.
- Regular Re-Screening: Every 1-2 years, based on the company's risk tolerance and policies.

For PEPs, who are generally considered high-risk due to their potential exposure to corruption and bribery risks, more frequent checks may apply: -

- PEP Re-Screening Frequency: Every 6 months.
- Transaction Monitoring: Continuous, with automated systems flagging any suspicious or large transactions for further review.
- Periodic Review of Customer Profile: Quarterly, to ensure that all information is up-to-date and any changes in circumstances are identified promptly.

Moreover, the Company conducts the verification through the use of 3rd party providers; collect additional information when establishing the identity of the Player by using additional documentation and information.

When undertaking additional CDD measures on PEPs, their family members or persons known as close associates, the Company shall apply all the EDD measures, such as:

- a) obtaining senior management approval
- b) taking adequate measures to establish the source of wealth and funds involved c) conducting enhanced ongoing monitoring
- d) EDD measures for long-term insurance business.

The Company will also establish, record, maintain and operate appropriate procedures and controls for requiring the approval of senior management:

- (a) before any new customer relationship is established with the PEP or;
- (b) before any ongoing customer relationship is established with the PEP

In addition, the Company will take reasonable measures to establish the source of wealth of PEPs within thirty days of the (€2000) - (4.000 NAF) threshold being met, as well as carry out regular ongoing and effective enhanced monitoring of PEPs at least every 6 months.

Where the PEP fails to provide sufficient data or documentation needed, any existing relationship with the said PEP will be terminated by closing the account and available funds will be remitted to the PEP.

Internal and/or external systems will be used to monitor play for signs of fraud, and these players are flagged accordingly for investigation.

4. User Education and Support/ Player management

4.1 Responsible Gambling

1. Users will be provided with educational resources on responsible gambling during onboarding.
2. Self-exclusion options and deposit limits will be available in the user's account settings.
3. Regular email campaigns and in-app notifications will remind users of responsible gambling practices and available tools.

4.2 Customer Support

1. A dedicated team will assist users with onboarding, including KYC verification and technical issues.
2. Support will be available 24/7 via live chat and email.

3. Escalation procedures will ensure prompt resolution of high-priority issues, such as account suspensions or transaction disputes.

4.3 Player management account

1. The Player Management is part of a Player Account Management (PAM) system or casino management software used internally by WILLX N.V. and includes the following:
 - Tracks player profiles (name/ surname, age, identification documents, gameplay patterns)
 - Manages deposit limits, bonus eligibility, and responsible gaming measures
 - Records wins/losses, game preferences, and promotional offers
 - Supports anti-money laundering (AML)

PAM systems are critical for:

- Secure account creation
- Payment gateway integration
- Loyalty & bonus program management
- Analytics on player behavior
- Compliance with gambling regulations

Company's Player Account Management (PAM), provides a comprehensive player account overview. Moreover, provides the access in order to monitor player betting and session activity, review received bonuses, check player balances, manage self-exclusions and account restrictions and monitor all financial transactions.

5. Review and Updates

1. This onboarding policy will be reviewed quarterly to incorporate regulatory changes and emerging best practices in fraud prevention.
2. Updates to the policy will be communicated to users via email and prominently displayed on the platform.
3. Feedback mechanisms will allow users to report issues or suggest improvements to the onboarding process.