

Proyecto PRO B.V.

Technical Project

Table of contents	
Chapter	Page
USER REGISTRATION, GAMING ACCOUNT AND METHOD OF PAYMENT	3
<u>PROTECTION OF PERSONAL DATA</u>	10
<u>REPORTING AND CONTROL SYSTEM</u>	14
<u>RESPONSIBLE GAMING</u>	15

1.USER REGISTRATION, GAMING ACCOUNT AND METHOD OF PAYMENT

User Registration

A player must be registered in order to participate in gaming. The consolidation of the operator's user registration will constitute the players' registration.

The user registration consists of both the verification phase of the information provided by the player and the player's identification phase.

The user registration must verify the information from the player ensuring he is not included as a person prohibited from gambling.

A person would not be allowed to participate in gaming when included under the subjective prohibitions:

- a) Minors and those incapacitated legally or by court decision
- b) Shareholders, owners, participants, or significant rights holders of the game operator, its personnel and employees directly involved in the game development, as well as their spouses or co-inhabitants, primary ascendants, and descendants, regardless if the participation is direct or indirect via third-party persons or entities.
- c) Athletes, trainers, or other direct participants or organizers involved in the sports development or activity on which the wager is being placed.
- d) The participating or organizing sports entities managers of the sports activity on which the wager is being placed.
- e) Judges or referees that participate in the sport's development or activity on which the wager is being placed, as well as those that resolve any decisions against them.
- f) IPLYC personnel and officials.

We will ensure the identity of the players by using one of the following procedures:

- When the method of payment to be used by the player provides the required information to ensure the person's identity, identification will be made automatically

Examples of such payment methods include bank transfers and credit/debit cards. The IPLYC shall authorize the methods proposed by the operator. (per regulator clarification on 05/16/19)

- When the method of payment to be used by the player does not allow the person's identification, other manual identification methods will be employed by using a service for identification of the player's information that is sufficient to determine the veracity of the registration. This service may be provided by third-parties that provide professional services for verification of identity

The manual identification process is an internal operator control.

A player may commence play on the platform once the user registration process is completed successfully.

Depending on the jurisdiction, the user registration will include the following information:

- First and last name
- Type of document and number
- Residence address
- CUIL/CUIT
- Date of birth
- Gender
- E-mail address
- Telephone (Optional)

We will record and retain the totality of all actions, consultations and requirements, which were realized for the identification and verification of information provided by the applicant, as well as the documents that were received or used for that purpose. Additionally, they must record the date and time (hour and minute) of these transactions.

This information shall be retained together with the information corresponding to the user registration for a period of not less than five (5) years after the closing of the user account.

Verification after registration.

We will establish the procedures and mechanisms necessary to ensure that the same player does not have several user accounts in their platform

We will be responsible for the authenticity and periodic review of the information recorded in the user registration, in the terms established in this document

Periodic review of user registration: We will establish a technical procedure, that allows a periodic review of the user registration in the terms established in this document

The frequency of the previously mentioned reviews shall be no less than twice monthly, and for the verification of auto-exclusion, either temporary or permanent, this review will be conducted at the beginning of each session

In case a user registration is not valid, the account shall be suspended. We shall retain all data from the canceled user registrations. The record must detail the time of cancellation and the reason.

Gaming account

Once the registration process has been completed, the player will be assigned a unique user identification. Access to the user registration and the gaming account shall be exclusively reserved for the player who is the registration holder.

Suspension for inactivity

We will suspend the player's gaming account when the period of inactivity exceeds twelve (12) months

Provisional suspension of the gaming account.

We will, with prior notification to the IPLYC, provisionally suspend a player that, in their judgment, has exhibited collusive or fraudulent behavior, or has permitted the use of their account by third parties, until the facts are proven.

Closing of gaming accounts.

When the account has been suspended for twelve (12) months, it will be closed.

When the gaming account is closed, the player must register again to be admitted to the platform.

Functionality of the gaming account

Each user registration shall be linked to a unique gaming account.

The gaming account shall reflect all transactions that involve a change of the player's balance, such as deposits made by the player, game participation fees, payment for bonuses offered by us, and the prizes obtained by the player.

The gaming account shall be denominated in the legal currency of each jurisdiction and the US Dollar alternatively.

All corrections, cancellations, or adjustments shall be reflected in independent entries, which in any case must not erase the original corrected, canceled, or adjusted transaction.

The wagers that once formalized have been cancelled by us will be registered, clearly indicating the reason for their cancellation.

User authentication and password policy

Access to the user registration must have a security mechanism to authenticate the user in the platform.

User authentication will be realized through the use of passwords.

The system must not utilize cookies or other mechanisms to prevent user authentication or password entry

The system will not allow the storage of passwords to bypass its entry by the user.

Access registration

When a user opens or closes a session, the event information will be maintained. The following will be safeguarded:

- Gaming account
- Date and time (open/close)
- IP
- Player device
- Localization of the user terminal

Information to the player on his last connection.

Once the user is authenticated, the system will display the date and time of his last access.

History

The player will be provided the balance of his gaming account in real-time, and the record of all participation or games played in the last thirty (30) days, as a minimum.

The player may obtain a summary in real time for a period of one year, of all activity in his gaming account to include:

- initial balance
- sum of deposits made
- sum of withdrawals made
- sum of the fees for the cost of participation in games
- sum of the payments for the possible bonuses accepted by the player and for the prizes obtained
- the final balance

Session configuration

The user will be able to configure limits.

The configuration for notifications, or the automatic end of the session will be distinguished.

Modification to the limits will be maintained with the user registration.

In the event the limit of time or credit is reached during the development of an unfinished game, the user may opt to continue the game or retire but must not be able to start another game.

Unfinished games will be terminated before another game can start.

Promotional Offers

We offer many different promotions where the customers usually need to deposit or bet or both to qualify. Some of these promotions are automated and for those we do display, on the Promotions Details Page, a customer's progress in qualifying for the promotion i.e. you have bet 5 U\$, you need to bet another 5 U\$. Only some promotions are automated (the majority of acquisition promotions, many CRM promos and less than half of retention promotions).

The customer can see their progress by looking at 'My Bets' or 'Transaction History' to add up the total of the deposits and bets made during the qualifying period. Our promotions strategy includes automating as many of the most used promotions, so we continually look to provide customers with the best experiences.

User balance

Denomination of gaming account: the unit of currency of the gaming account will be the legal currency of jurisdiction, and U\$ alternatively.

Prohibition of transfers between participants.

Transfers between gaming accounts associated with different user registrations will not be available.

Limits on deposits and duration of play.

We will maintain a register with modifications to the limits on deposits and duration of play detailed per user registration. The date and the reason for the modification will be included.

There will be a notation if the modification was requested by the player or established by us.

Credit balance.

The player will not be able to bet without a sufficient credit balance.

Methods of payment

We will maintain a detailed account of each deposit or withdrawal transaction as well as the information associated with each transaction.

Payment Methods

All deposits and withdrawals will be processed using secure and verified payment methods that comply with regulatory requirements. We will maintain a detailed account of each transaction, including the associated user information, timestamps, and verification logs.

Deposit Methods and Processing Times

Payment Method	Processing Time
Bank Transfer	1-3 business days
Credit/Debit Cards (Visa, Mastercard)	Instant to 24 hours
E-Wallets (Skrill, Neteller, PayPal)	Instant
Cryptocurrencies (Bitcoin, Ethereum)	10-30 minutes (subject to network congestion)
Prepaid Cards (Paysafecard, Neosurf)	Instant
Mobile Payments	Instant

Withdrawal Methods and Processing Times

Payment Method	Processing Time
Bank Transfer	2-5 business days
Credit/Debit Cards (Visa, Mastercard)	1-3 business days
E-Wallets (Skrill, Neteller, PayPal)	24 hours
Cryptocurrencies (Bitcoin, Ethereum)	10-60 minutes (subject to network verification)
Prepaid Cards (Paysafecard, Neosurf)	Not Available
Mobile Payments	1-2 business days

Additional Payment Guidelines

- **Processing Hours:** Withdrawals are processed during business hours (Monday-Friday, 9:00 AM - 6:00 PM UTC). Requests made outside these hours will be processed the next business day.
- **Verification Delays:** Withdrawals may be subject to additional verification checks, which can extend processing times.

- **Transaction Limits:** Minimum and maximum limits per transaction are defined based on the jurisdiction and selected payment method.
- **Pending Withdrawals:** If a withdrawal remains unprocessed beyond the expected timeframe, players should contact customer support for escalation.
- **Currency Conversions:** If a player deposits or withdraws in a currency different from the platform's primary currency, exchange rates and fees will apply.

Transfer of funds.

We will set a procedure to arrange for a method of payment that is applicable to the transfer of funds in a maximum period of 48 hours.

Control procedure for payment and cashout transactions.

We will implement a procedure to compare the payment and cashout transactions against the entries in the gaming account or game software, which will include:

- The gaming account associated with the user registration in a status other than active does not perform improper activities
- The verification that the amounts of deposits and withdrawals correspond to the amounts of the transactions realized by the method of payment
- The verification that no deposits are made by the players over each of the fixed limits on the deposit
- The verification that withdrawals are conducted within a maximum period of 48 hours, except for foreseeable cases with prior notification to the IPLYC
- The procedure shall be executed monthly, as a minimum

2. PROTECTION OF PERSONAL DATA

Protection of data

We will implement the security measures established in the respective country regulations for the protection of data on the archives and their handling, and comply with the obligation of secrecy provided in said regulations.

Privacy policy

The privacy policy will be available on the game platform.

The player will need to accept the privacy policy to complete the registration.

The platform will register the player's acceptance and the content of the privacy policy or a link to its context.

There will be a notification to the user for each modification of the privacy policy.

INFORMATION SYSTEMS SECURITY

Security requirements

We will guarantee the conditions of physical and logical security for the entire technical gaming system, in a way that ensures the integrity and availability of the game and the information generated and managed, produced from the operation.

To this end, we will implement a security management system that follows the guidelines of standards ISO/IEC 27002:2022 27001:2013, and 27005:2011, GLI 27 and observes the policies, processes, procedures, and controls that safeguard the critical elements described in the following items and are focused on the following aspects of the operation of the technical gaming system:

- Guarantee the integrity, confidentiality, and privacy of data and information transmitted between the remote connection devices and the technical gaming system that is transported in the public network of the internet, and between the various components of the system in the operator's private network.
- Guarantee the integrity, confidentiality, and privacy of data and information processed and stored in the technical gaming system
- Maintain in an online database or its history back-up, all control events, results, and wager information generated in the technical gaming system for the duration of the licensee's contract
- Mitigate the operational and technological risks of the technical gaming system that may arise from threats and vulnerabilities of each of the components of the system

- Any others we will deem necessary to guarantee the proper development of the game and its operation

Critical components

Critical components are those elements that require security management, as their impact on the development of the game is important.

The following are critical elements:

- The user account, the gaming account, and the processing of the method of payment: the components of the technical gaming system that store, manipulate, or transmit the player's sensitive information, such as personal, authentication, or financial data, and data stored according to the status of the game, wagers and their results
- In the random number generator: the components of the technical gaming system that transmit or process random numbers utilized for the outcome of the games and the integration of the RNG results in the game logic
- The connections with the IPLYC and the communication networks that transmit the player's sensitive information
- The reporting and control system: Redundant database (RBD)
- The points of access and the communications to and from the critical components previously mentioned

Security management of the technical gaming system

We will implement a security management system, to specifically safeguard the critical components described in the previous section. Security procedures will be established to implement specific security measures, starting with a risk assessment, performing scheduled periodic reviews, and conduct reviews due to any significant changes

Risk management

For risk management, we will use the standard ISO/IEC 27005:2011 as a guide to implement the processes that facilitate the evaluation, analysis, handling, and acceptance of the risks that could affect the technical gaming system. We will maintain the registers and evidence required for compliance with appropriate risk management during the auditing process

Security policy

We will have a security procedure that will be communicated in its entirety to his employees, and if applicable to supporting external entities

Security of player communications

Authentication mechanisms will be in place, which allow the identification of the player in the game system, and conversely, allow the player to identify the gaming system and establish the systems and mechanisms that guarantee the confidentiality of player communications with the technical gaming systems, and in particular with the gaming central unit and its replica.

Communications will be encrypted in the event of transmission of personal data (user registration) or financial data (gaming account)

In regards to communications, we will adopt the necessary measures to guarantee security and non-repudiation in the case of transmission of personal or financial data, and transactions when participating in the games

Security of human resources and third parties

Our security plan for personnel must include active training and will be considered for the management of personnel employment, paying particular attention to permissions to access information and critical elements.

When we require the services of providers that need access, processing, communication, or handling of information, or access to installations, products, or services related to gaming, the third parties must comply with all security requirements applicable to other technical users

Plan for the prevention of loss of information

We will have a plan available that ensures no loss of data or transactions that affect or could affect the development of the games, the rights of the participants, or public interest and indicates the risk assumed by our company.

Our infrastructure will allow us to:

- Backup copies that will be maintained in an adequate place separate from the data being safeguarded.
- Backup copies that will be protected against unauthorized access through security measures equivalent to the information being safeguarded

We will have a documented procedure for action in the event of loss of information, which will include the mechanisms to respond to user claims, game continuation of interrupted games or wagers, and any other situations that may arise.

Management of business continuity

We will have a business continuity plan for maintaining the gaming operations during a disaster, which includes the technical, human, and organizational measures required to ensure the continuity of service and a redundant gaming central unit that allows normal development of the activities

The business continuity plan will establish one or more recovery scenarios, each of them indicating the services recovered and the maximum period of time these would remain operative.

We will consider the following scenarios within the plan:

- Access of the players to the user registration and gaming accounts, with the option to check on their balances and activity on their associated gaming accounts. The maximum amount of time to resume providing these services will be 4 business days
- Player option to withdraw funds. The maximum amount of time to resume providing these services will be 5 business days

- Continuation of incomplete games or pending wagers, and payment for valid prizes obtained.
The maximum amount of time to resume providing these services will be thirty (30) days
- Complete reestablishment of all services
- We will adapt his infrastructure and processes, and implement the necessary measures to comply with the objectives established in their business continuity plan
- In the event of a disaster, we will inform immediately, providing an estimation of its impact and the estimated period for recovery

3. REPORTING AND CONTROL SYSTEM

The required reports will be generated in PDF format and in any of the following standard formats for ease of use: csv, json, xml, etc.

The content of the reports will include the following information:

- Registered data from the players and their gaming accounts, initial balance, deposits, withdrawals, wagers per game, payment or credit for prizes obtained during the game, bonus converted to credit, ending balance.
- Accounting data from the game, which includes as a minimum, for each valid game or confirmed play, game play voided or canceled by the operator, gameplay denied, wagers made by the players, and the transactions of payment or credit for prizes realized by the operator
- Transactions on game events, which include the games played, games voided, and prizes obtained, per tournament, game, or session.
- Transactions on user registration and gaming accounts, which include as a minimum, registration and opening of the account, data provided by the players, results of verification of data and identification, acceptance of the terms and conditions, modification of account parameters, financial transactions in the gaming account and closing of the account
- Accounting information, on money wagered and played by the participants and payment of prizes
- Participant claims

4. RESPONSIBLE GAMING

Prevention of compulsive gambling and auto-exclusion

Enhancements in Prevention of Compulsive Gambling and Auto-Exclusion

To strengthen the focus on **responsible gaming**, proactive strategies have been implemented to detect and prevent problematic behavior before it escalates.

Self-Exclusion and Limitations

- Players can voluntarily set **restrictions** on their gaming activity, including:
 - **Deposit Limits** (daily, weekly, or monthly)
 - **Loss Limits** (caps on net losses per session or time frame)
 - **Wager Limits** (maximum bet per game or period)
 - **Session Time Limits** (automatic log-out after exceeding the set duration)
 - **Self-Exclusion** (temporary or permanent exclusion requests)
- **Proactive Auto-Exclusion Mechanism:**
 - Players flagged for **repeated risky behavior** will be temporarily suspended for a review.
 - Players showing signs of distress will receive **automated responsible gaming messages** and **optional intervention from human agents**.
 - A dedicated **Self-Exclusion Support Team** will be available 24/7.

Real-Time Player Risk Scoring System

- A **Risk Score** is assigned to each player based on their real-time behavior using a **traffic-light system**:
 - **Green (Low Risk)**: Normal gambling behavior.
 - **Yellow (Medium Risk)**: Warning signs detected; system sends **responsible gaming notifications**.
 - **Red (High Risk)**: Immediate **cool-down period**, and a **Responsible Gaming team member** will contact the player directly.
- **Mandatory Intervention for High-Risk Players:**
 - A **personalized risk assessment** will be conducted.
 - Players must agree to a controlled play plan or face **immediate exclusion**.

Cross-Platform Data Integration

- Integrates with **third-party databases** (e.g., national self-exclusion registries, partner casino networks) to prevent players from bypassing restrictions by registering under new identities.

Responsible Gaming Notifications & Reality Checks

- Pop-up alerts every **60 minutes** displaying session duration, total bets, and net wins/losses.

- Players exceeding **three consecutive hours of play** will receive a **mandatory break message** before continuing.
- **Gamification Prevention:** Players who frequently chase losses will be temporarily blocked from high-volatility games.

Responsible Gaming Helpline & External Support

- **24/7 support** available to players, including:
 - **Live Chat Support Team** trained in gambling addiction counseling.
 - Direct referrals to **recognized responsible gaming organizations**.
 - Option to request **financial spending reports** for self-auditing purposes.

We will establish measures for the prevention and detection of compulsive gambling. Such measures will include:

- a) a mechanism so that each participant can, either at the time of registration or at the beginning of each session, configure their access to the game platform, establishing temporary limits or time intervals in which access would be denied, as well as establishing caps or limits on the deposits, per session/day/month, which we will immediately apply
- b) issuing alerts -visual and sound- informing the user that he started the session more than three (3) hours ago, and repeating the same on an hourly basis, and a notification at the end of each session to inform: the duration of play from the start of the session, types of games played, current status of his account, amount wagered, and prizes obtained
- c) and permanently display in a conspicuous place a notice advising of the risks of gaming and the means of help, including the procedure of auto-exclusion

Additionally, we will utilize mechanisms that detect behavior that denotes the presence of pathological or compulsive gambling, through establishing player tracking (for example, frequency of play, amount of wagers, increment/elimination of limits) that generates alerts

Prevention of fraud and money laundering

To strengthen fraud prevention and **Anti-Money Laundering (AML) compliance**, we have expanded our measures by integrating **specific risk thresholds, real-time monitoring tools, and automated reporting systems**. These improvements ensure compliance with AML regulations and proactively detect fraudulent activities.

Risk-Based Monitoring & Automated Alerts

- Transactions will be continuously **monitored using AI-driven algorithms** to detect suspicious patterns.
- **Automated alerts** will be triggered when predefined risk thresholds are met, including:

- **Unusual deposit patterns** (e.g., frequent high-value deposits without corresponding gameplay activity).
- **Multiple withdrawal requests** within short time frames.
- **Abnormal betting behavior**, such as consistently low-risk bets with no variance.
- **Deposits followed by immediate withdrawals** without wagering (commonly associated with money laundering attempts).
- **Usage of multiple accounts from the same IP/device** to exploit bonus abuse or commit fraud.

Transaction Thresholds & KYC Reinforcement

- A **tiered risk assessment system** will be applied to transactions based on jurisdictional AML regulations:
 - **Low-risk players:** Standard KYC verification applies.
 - **Medium-risk players:** Additional document verification required for transactions exceeding regulatory thresholds.
 - **High-risk players:** Enhanced Due Diligence (EDD) applies for transactions exceeding predefined limits.
- **Threshold Limits for Review & Escalation:**
 - **Single transaction review:** Deposits or withdrawals exceeding \$5,000 (or equivalent in jurisdictional currency).
 - **Cumulative transaction review:** Multiple transactions exceeding \$10,000 in a 30-day period.
 - **High-risk jurisdictions:** Enhanced scrutiny for transactions originating from or directed to flagged jurisdictions under AML directives.

AML Policy Compliance & Reporting

- All AML-related procedures align with **local and international regulatory frameworks**, including:
 - **Financial Action Task Force (FATF) Recommendations**
 - **EU Anti-Money Laundering Directives (AMLD)**
 - **Bank Secrecy Act (BSA) and USA PATRIOT Act**
 - **Other applicable national AML laws**
- Any **suspicious activity reports (SARs)** will be generated and submitted to the appropriate regulatory authorities, in accordance with AML compliance policies.

Cross-Platform Fraud Prevention & Data Sharing

- Integrates with **third-party fraud detection databases** to flag known fraudulent accounts.
- **Multi-account detection** mechanisms prevent users from creating duplicate profiles to exploit promotions or circumvent limits.
- Transaction monitoring systems **cross-check data across payment methods, geolocations, and betting behavior** to identify coordinated fraudulent activity.

Real-Time Identity Verification & Geolocation Checks

- Uses **real-time KYC (Know Your Customer)** and **AI-driven identity verification** to prevent fake accounts and identity fraud.
- **Geolocation tracking** ensures transactions originate from permitted jurisdictions and blocks access from flagged locations.
- **IP and device fingerprinting** technology detects and prevents account sharing or unauthorized logins.

Collaboration with Financial Institutions & Regulators

- **Continuous collaboration with financial partners and regulatory bodies** to improve transaction monitoring.
- **Regular audits and risk assessments** to align with evolving AML standards.
- Participation in **AML intelligence-sharing networks** to stay ahead of emerging fraud trends.

We will have procedures for the detection of fraud and money laundering. The procedures must include the prompt notification of suspicious actions to the competent public organisms for their investigation.

For the live betting games, we will have available measures to mitigate the risk that some players may gain an advantage over others by wagering with information on a certain result or after an incident that may fundamentally alter the probabilities of the wager

Participant claims

We will make available to the participants, and any other person who may be affected by the operator's performance, a system of customer service that focuses on the resolution of claims, complaints, and suggestions

Such system must have access electronically via the website and/or game session, which must be easily accessible to interested parties, and we will record the claimant's information, date and time of receipt of the claims presented, as well as maintain a record of activities and games where the incident could have occurred

We will provide information to the user in a way that is certain, clear, and detailed concerning such a system of customer service, which must include: postal address and electronic alternatives where claims may be directed and, when applicable, standard formats; timelines for the submission and timelines for we will communicate their decision/ resolution

Customer service for the participants must be conducted free of charge and multilingual.

Timeline for claims:

1. Presentation: we will not establish a period lesser than thirty (30) days for the submission of claims, from the time the incident occurred subject to the claim

We will issue a communication to the claimant, which will acknowledge receipt of the claim and the period of time to make the decision to that effect

2. Resolution: we will resolve the claim and communicate it to the claimant within a period not greater than thirty (30) days, starting from the date that the claim was received