

OPERATIONAL MANUAL

Jazz Business Solution B.V.

2025

Contenido

Risk Assessment Policy	6
INTRODUCTION	6
1. MONEY LAUNDERING	6
1.1 What is Money Laundering?	6
2. AML RISK ASSESSMENT AND MITIGATION	7
2.1– General	7
2.2– Risk Management Strategy	8
Purpose.....	8
Tiers of AML Protocols Tier 1: Identity Verification.....	8
Tier 2: Source of Funds.....	8
Tier 3: Continuous Monitoring	8
Tier 4: Destination Confirmation.....	9
Detailed Descriptions	9
3- IDENTITY VERIFICATION (Tier 1).....	9
3.1- KYC POLICY	9
Know Your Client (KYC) Protocols Policy	9
Purpose.....	9
Objectives	9
Procedures.....	10
Preliminary Screening Customer Account Policy Account Ownership	11
Screening Process	11
Risk Detection	12
3.2 EDD (Enhanced Due Diligence Procedures).....	13
3.3 Politically Exposed Persons Policy	14

4– SOURCE OF FUNDS (Tier 2).....	15
4.1– General	15
4.2– Mitigation through Deposit Limits	16
5– CONTINUOUS MONITORING (Tier 3).....	16
5.1– Suspicious Conduct.....	17
5.2– Reports and Reporting.....	18
a. Significant Payment Reports (STRs)	18
b. Suspicious Activity Report (SARs).....	18
c. Sports Betting Reports.....	18
d. Casino Gaming Reports.....	18
e. Poker Security Reporting and Tools	19
6– DESTINATION CONFIRMATION (Tier 4)	19
Governing Payout Transaction Policy:	19
Exceptions and Enhanced Diligence:.....	19
Withdrawal Request Review:	20
7- EMPLOYEE DILIGENCE	20
7.1– Employee Screening	20
7.2– AML Training.....	20
7.3– Third Party Supplier Diligence.....	21
8– WIDER ENVIRONMENT	21
8.1 General	21
8.2– Market Changes.....	22
9 - CONCLUSION.....	22
Know Your Customer (KYC) Policy	23
1. Purpose of this Policy	23

2. Scope	23
3. Why KYC is Required	23
4. Information We Collect	24
5. Verification Process	24
6. Ongoing Monitoring	24
7. Data Protection	25
8. Player Responsibilities	25
9. Non-Compliance	25
10. Contact Us	25
Player Complaints Policy	27
1. What Is a Complaint?	27
2. Timeframe to Submit a Complaint	27
3. How to Submit a Complaint	27
4. How We Handle Complaints	27
All Other Complaints:	28
5. Escalation – Alternative Dispute Resolution (ADR)	28
Contact details for our ADR provider:	28
6. Record Keeping and Reporting	28
7. Your Legal Rights	29
8. Overview of Issues Covered	29
9. Contact Us	29
Security Policy	30
1. Account and Password Security	30
2. Data Protection and Privacy	30
3. Platform Security and Infrastructure	30

4. Incident Reporting and Response	31
5. Secure Crypto Operations	31
6. Ongoing Monitoring and Audits	31
7. Disclaimer s Limitation of Liability	32
Responsible Gaming Policy	33
1. Your Safety and Our Commitment.....	33
2. Age Verification and Eligibility.....	33
3. Responsible Gaming Tools.....	33
4. Self-Assessment Tools	34
5. Identification of Problem Gambling	34
6. Account Suspension and Breaks	34
7. Advertising and Marketing Practices.....	35
8. Support Services and Resources	35
9. Policy Review and Oversight	35

Risk Assessment Policy

INTRODUCTION

Jazz Business Solutions B.V. operates an online gaming enterprise and is committed to the implementation of robust KYC (Know Your Customer) protocols and operational monitoring/reporting mechanisms to mitigate risks that could negatively impact the organization. Jazz Business Solutions B.V. (hereinafter referred to as the “Company”) has established the following general principles to reasonably mitigate Anti-Money Laundering (AML) exposure, considering the source and nature of its various business channels and targeted markets:

This Risk Assessment (hereinafter referred to as the “Policy”) is designed to identify and address any real or perceived risk of money laundering and terrorism financing posed by the Company's activities as it conducts operations in the online gaming sector.

1. MONEY LAUNDERING

1.1 What is Money Laundering?

The Regulations of the GCB for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, have defined Money Laundering as:

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

Money Laundering consists of three phases:

- o **Placement:** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requesting for

pay out and inserting funds into gaming machines and immediately claiming those funds as credits;

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

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

2. AML RISK ASSESSMENT AND MITIGATION

2.1– General

The Company has implemented necessary and effective measures to reasonably mitigate any money laundering risk associated with its services and various transactional processes:

- The identity of players is verified through appropriate KYC protocols before permitting any payout transactions and whenever possible, considering the nature of the payment method.
- All deposits are received from verified sources associated with the player's identity.
- All payout transactions are verifiably issued only to the account holder.
- Where possible, payout transactions are restricted to the transaction method used for the initial deposit (i.e., funds are paid out only to the card, wallet, or other deposit method from which the deposit was received).
- Cash transactions are prohibited, both as deposit and payout methods.
- Credit is not extended to players under any circumstances other than through bonus programs.

- Inter-account transfers of funds or tokens, poker chips, or any redeemable coupon or credit of any kind are not permitted.
- Player activity is actively monitored daily for suspicious activity that could result in an effective transfer of funds from one player to another, such as "chip dumping."
- All bet or wager transactions are in electronic format, recorded, maintained, and auditable.

2.2– Risk Management Strategy

Purpose

The Anti-Money Laundering (AML) protocols of the Company are structured around four critical tiers. These tiers, collectively implemented, are designed to reasonably mitigate any potential AML risks associated with the Company's operations.

Tiers of AML Protocols Tier 1: Identity Verification

- **Objective:** Verify the identity of the account holder.
- **Procedure:** Ensure that the identity verification process is completed as soon as practicable, but strictly before any withdrawal or payout is made. This is to mitigate AML risks by confirming that the account holder's identity is valid.

Tier 2: Source of Funds

- **Objective:** Confirm the legitimacy of the funds deposited.
- **Procedure:** Verify that the funds deposited into the account are from a source that can be confirmed as belonging to the account holder, whenever possible. This process considers the nature of the deposit method to ensure the source of funds is legitimate.

Tier 3: Continuous Monitoring

- **Objective:** Monitor account activity for suspicious behavior.

- **Procedure:** Continuously observe account activities for any potentially suspicious patterns, behaviors, or transactions. Examples include attempted chip dumping or player collusion. This ongoing monitoring helps in identifying and mitigating risks promptly.

Tier 4: Destination Confirmation

- **Objective:** Ensure payouts are made to legitimate destinations.
- **Procedure:** Whenever possible, verify that any payout transactions are directed to a destination that can be confirmed as belonging to the account holder. This step ensures that the funds are transferred securely to the rightful owner.

Detailed Descriptions

Each tier mentioned above is elaborated in detail in the subsequent sections of this policy document. This ensures a comprehensive understanding and implementation of each step to maintain the integrity of the Company's AML measures.

3- IDENTITY VERIFICATION (Tier 1)

3.1- KYC POLICY

Know Your Client (KYC) Protocols Policy

Purpose

Effective and closely monitored Know Your Client (KYC) protocols are fundamental to mitigating Anti-Money Laundering (AML) risks. Customer due diligence is an essential process that enables the Company to identify its clients and service providers, and to verify their identities.

Objectives

The objectives of this policy are:

1. **Identity Validation:** To ensure that the identity of each client is verifiable and valid.

2. **Risk Assessment:** To determine whether the validated identity poses a heightened risk of fraud, terrorist financing, or AML activities.

Procedures

1. Customer Due Diligence (CDD):

- **Verification Process:** The Company will conduct thorough due diligence to verify the identity of each client. This involves collecting and examining identity documents and other relevant information to confirm the client's identity.
- **Risk Assessment:** Upon verifying the identity, the Company will assess the potential risks associated with the client. This includes evaluating the risk of fraud, terrorist financing, and AML activities.

2. Account Restrictions:

- **Inability to Complete Due Diligence:** If the Company is unable to complete the due diligence process for any reason, the affected account will be disabled. This means the account will be restricted from depositing funds or engaging in any gaming or wagering activities.
- **Implementation of Safeguards:** The Company may implement additional safeguards or procedures as necessary to mitigate risks until due diligence can be completed.

3. Re-enabling Accounts:

- **Verification Confirmation:** Once the client's identity has been verified and deemed valid, the account may be re-enabled.
- **Company Discretion:** The decision to re-enable the account will be at the sole discretion of the Company, ensuring that all AML and KYC requirements are satisfactorily met.

Preliminary Screening Customer Account Policy Account Ownership

1. **Individual Accounts Only:** Customer accounts may only be held in the name of an individual. Corporations, partnerships, trusts, associations, or any other form of legal entity are prohibited from holding accounts.
2. **No Anonymous or Fictitious Accounts:** The Company shall not establish anonymous customer accounts or accounts under names it knows or reasonably suspects to be fictitious.

Account Registration

3. **Mandatory Details:** All individuals are required to provide their details upon sign-up with the Company system. Each individual is permitted to operate only a single account.

Screening Process

4. **Preliminary Screening:** Upon creation of a new account, a preliminary screening, both automated and manual, is conducted to identify potentially linked or other suspect account activities. Third-party service providers such as Iovation significantly aid in the initial screening process. Information captured through these services includes:
 - Device IP (silently gathered) – also known as "device fingerprinting"
 - ISP
 - Geo-location
 - VPN/Proxy usage (silently gathered)
 - Customer information (name, address, date of birth)
 - Email address
 - Password
 - Security questions/answers
 - Acceptance of the Company's Terms and Conditions

Risk Detection

- **Information Utilization:** Capturing this information allows the Company to detect and screen for account holders who may:
 - o Create and/or access more than one account
 - o Have similar/identical information to other accounts
 - o Share the same device used to access accounts
 - o Share the same deposit/withdrawal instrument to fund the account
 - o Exhibit other suspicious activity such as appearing on a PEPs list
- **Investigation and Risk Mitigation**
 - **Automated Alerts and Investigation:** If any screening identifies potential issues, the investigation team is automatically notified to investigate and apply applicable business rules. These business rules may result in various potential risk mitigation steps, including:
 - o Closure of the account
 - o Escalation to the Fraud team for enhanced diligence
 - o Limitation of deposit or withdrawal methods
 - o Imposition of deposit limits
 - This policy ensures that all customer accounts are managed with high standards of security and due diligence to mitigate potential risks associated with account activities.

3.2 EDD (Enhanced Due Diligence Procedures)

In situations where customer relationships present heightened AML or fraud risks, the Company will implement enhanced due diligence (EDD) procedures in addition to its regular customer due diligence protocols. The following outlines the steps involved:

1. Purpose of Enhanced Due Diligence: Enhanced due diligence is conducted to gather more comprehensive information about a potential customer, their personal and financial background, and the source of their funds. This process includes obtaining additional evidence to verify the customer's identity and ensuring thorough monitoring.

2. Enhanced Due Diligence Steps:

- *Additional Verification Evidence:* Obtaining further evidence to verify the customer's identity.
- *Particular Aspects Verification:* Verifying specific aspects of the customer's identity.
- *Source of Funds Verification:* Establishing the source of any funds of the customer.
- *Frequent Monitoring:* Conducting more frequent and extensive monitoring of the customer's activities.

3. Tools and Resources: The Company's fraud department agents utilize a variety of tools and databases provided by suppliers to verify submitted documentation, such as:

- Driver's Licenses
- Passports

4. Accepted Forms of Verification: The following documents are accepted as forms of verification:

- Marriage Certificate
- Name Change Certificate

- Driver's License
- Passport or other valid government-issued identification

5. *Circumstances Requiring Enhanced Due Diligence:* Enhanced due diligence is required in the following circumstances:

- *Geographic Risk:* The customer or potential customer is situated in a country or territory that does not apply or insufficiently applies the FATF Recommendations.
- *Politically Exposed Persons (PEPs):* The customer or potential customer is or appears to be a Politically Exposed Person.
- *Heightened Risk Perception:* Any other circumstances the Company reasonably perceives to pose a heightened risk of money laundering.

By adhering to these procedures, the Company aims to mitigate risks associated with AML and fraud, ensuring a secure and compliant operational environment.

3.3 Politically Exposed Persons Policy

A "Politically Exposed Person" (PEP) is an individual who currently holds or previously held a prominent public function in any country. This category encompasses a broad range of individuals, including heads of state, senior members of the judiciary, senior military officers, and immediate family members of such individuals.

Identification and Screening Process

During the initial screening process using third-party providers, the identity risk assessment reliably identifies Politically Exposed Persons. If an account is flagged as a potential match to a PEP list, it will be immediately blocked from making successful deposits pending further escalation and review.

Verification and Documentation

The Compliance Officer/MLRO will generate a report highlighting all new PEP notifications. This officer will then oversee client contact to verify, through documentation

or other means, whether the account holder is indeed the “matched” PEP. All documentation and feedback obtained during this verification process shall be promptly reported to the CEO and Managing Director.

Account Activation and Monitoring

No PEP account may be activated without the explicit authorization of the CEO, Managing Director, and Compliance Officer/MLRO. If reactivation is authorized, it will be subject to additional constraints or enhanced monitoring as mandated by the CEO, Managing Director, and Compliance Officer.

By adhering to these procedures, the Company ensures thorough scrutiny and due diligence in handling accounts associated with Politically Exposed Persons, thereby mitigating potential risks related to money laundering and other illicit activities.

4– SOURCE OF FUNDS (Tier 2)

4.1– General

Upon validating the identity of the account holder through either standard or enhanced due diligence, the next step involves ensuring that the source of the funds can be attributed to the validated identity, considering the method of deposit used.

To participate in gaming activities on the Company’s platform, customers must first deposit funds into their accounts. The Company offers various deposit options to ensure a seamless customer experience while fulfilling its customer due diligence (CDD) obligations:

a. Credit Cards

Credit cards can only be used if the name on the card matches the name on the account; otherwise, the transaction will be denied. If necessary, the Company may request the player to provide evidence of possession and ownership of the credit card. Transactions

require 'Verified By Visa' or 'MasterCard SecureCode' processes and this applies to refillable credit cards as well.

b. Wire Transfers and Direct Deposit Transfers

These methods require the source of funds to be an account or credit facility in the customer's name, which has been subjected to the KYC processes of the bank or applicable card issuer. These institutions and issuers are under stringent regulatory oversight and AML compliance requirements. Therefore, the Company assumes their KYC processes to be reliable for its operations.

c. Cryptocurrencies

With advancements in monitoring tools such as OXT.me and KYCP.org, cryptocurrency transactions can now be thoroughly analyzed. The Company employs blockchain experts to keep staff updated on the latest developments in the crypto world. These methods and reports assist in detecting shared wallets and other suspicious activities.

4.2– Mitigation through Deposit Limits

The Company targets casual, recreational bettors or players, operating a "retail" gaming enterprise. As an additional measure to mitigate AML and fraud risks (and to help prevent problem gambling), the Company imposes deposit limits on each available deposit method.

These limits are practical given the nature of the Company's target clientele and serve as a further barrier against money laundering schemes. Even without other safeguards, these limits make significant money laundering efforts logistically impractical.

If a customer reaches their deposit limit, they may contact Customer Service to request a limit increase or a one-time bypass. These requests are reviewed by a supervisor, and the client must submit additional documentation or information to confirm their identity and source of funds.

5– CONTINUOUS MONITORING (Tier 3)

This section addresses the continuous account monitoring and overview process designed to mitigate the risk of fraudulent conduct or the covert transfer of funds between

account holders (e.g., “chip dumping”). The Company is committed to ongoing monitoring of existing customer relationships and accounts, including:

- Reviewing identification data to ensure they remain current and relevant, especially for high-risk registered customers.
- Ensuring the proper recording and storage of identification data to facilitate continuous monitoring of each customer relationship.
- Scrutinizing transactions to ensure they align with the Company’s knowledge of the registered customer and their risk profile.

Several daily and weekly reports are generated to assist in detecting and analyzing suspicious activities from individual accounts or groups of accounts.

5.1– Suspicious Conduct

Suspicious activity cannot be exhaustively defined, but the following instances shall be investigated by the Fraud personnel, potentially constituting suspicious activity under this Policy (many reports will assist in detecting these cases):

- Suspicious play or financial activity by the customer.
- Deposits made by the customer without subsequent wagering over a significant period.
- Apparent “chip dumping,” collusion with other account holders, or other suspect behavior.
- Unusual transaction patterns or activities lacking apparent economic or lawful purposes.
- Attempts to deposit unusually large amounts of money.
- Use of deposit options not in the customer's name.

All suspicious conduct shall be immediately escalated to the Fraud Department and, if necessary, brought to the attention of the Compliance Officer without delay. Failure to

report any such case in accordance with the designated escalation process will result in disciplinary action, potentially leading to termination of employment or engagement. The Compliance Officer/MLRO will promptly investigate all reported cases and determine if a reporting requirement is triggered. The findings and recommended remedial actions will be documented and reported to the CEO.

5.2– Reports and Reporting

The following reports are generated daily or weekly for review and analysis by the appropriate department. Other reports require the Compliance Officer/MLRO or an authorized individual to compile and submit to the Regulator:

a. Significant Payment Reports (STRs)

The Company maintains an automated system to identify all account withdrawals exceeding a specific amount within a rolling 30-day period. Reports are generated within 48 hours of payment and submitted to the relevant Regulator.

b. Suspicious Activity Report (SARs)

The Company implements an automated system to identify accounts that may exhibit suspicious activity, including unusual gaming or transactional behavior. SARs are filed by the Compliance Officer/MLRO or an authorized individual and submitted to the Regulator.

c. Sports Betting Reports

Effective controls monitor and track customer activity in sports betting. Automated controls prevent customers from betting on both sides of an event, using multiple accounts, and participating in betting syndicates. Daily reports help identify potential violations of the Company's Terms and Conditions, leading to appropriate account actions.

d. Casino Gaming Reports

The Company's security and fraud prevention tools track all financial and gaming transactions. Daily reports assist in identifying players exploiting system vulnerabilities, leading to appropriate account actions.

e. **Poker Security Reporting and Tools**

The Company monitors online poker play to prevent money laundering and ensure fair play using tools such as:

- **Collusion Analyzer:** Flags accounts for potential collusive activity in ring games, based on various gameplay metrics.
- **Bot Detection:** Identifies accounts using third-party software, flagging them for review.
- **Bonus Abuse Reports:** Ensures compliance with bonus terms and detects abuse through referral incentives.

In cases where accounts are flagged for fraud, illicit activity, or other concerns, accounts are disabled and reviewed by the Poker Security, Fraud, and Compliance teams for appropriate action. If collusion is confirmed, funds are redistributed to affected accounts, and cheaters' accounts are disabled to prevent new account creation.

6– DESTINATION CONFIRMATION (Tier 4)

The Company's AML/CTF risk mitigation strategy ensures that payout transactions are directed to a destination associated with the verified account holder identity.

Governing Payout Transaction Policy:

- Payouts are processed back to the original transaction vehicle from which the initial deposit was made whenever feasible (e.g., payouts are credited back to the same credit card used for the initial deposit). This practice ensures that both deposits and payouts are linked to the verified individual, significantly reducing AML risk for the organization.

Exceptions and Enhanced Diligence:

- Deviations from this policy are permitted only on an exceptional basis. If the transaction vehicle cannot receive the credit transaction (e.g., MasterCard credit cards, which do not allow crediting), enhanced diligence is required before processing such a payout.

- In such cases, account holders must submit verifying documentation to validate their identity, the initial deposit vehicle, and the payout destination vehicle.

Withdrawal Request Review:

- Prior to processing any withdrawal request by the account holder, the generated funds are reviewed by the appropriate department. This review, applicable across all channels (Sports Betting, Casino, Poker), ensures that funds were legitimately won or generated and that all applicable bonus terms have been respected.

This structured approach to AML/CTF risk management ensures a robust framework for verifying the legitimacy of transactions and protecting the organization from potential risks.

7- EMPLOYEE DILIGENCE

7.1– Employee Screening

All employees and staff members of business affiliates or service providers involved in Company tasks undergo comprehensive screening before being hired or appointed. This includes an extensive background check and may involve credit and criminal record checks prior to any offer of employment.

7.2– AML Training

Specific training protocols will be provided to the following functional groups:

- Frontline Staff (customer service)
- Fraud/Investigation employees
- Financial Services
- Management/Senior Management

The Compliance Officer/MLRO is responsible for ensuring that training modules effectively communicate the requirements of this Policy. Training will cover the identification and reporting of transactions that must be reported to the Compliance

Officer/MLRO, and examples of different forms of money laundering schemes that could exploit the Company's business.

Training participants will be assessed to ensure understanding, and AML training sessions will be conducted at least once every twelve months. The Compliance Officer will maintain records of employee attendance and assessment results, which will be retained for a minimum of six years.

7.3– Third Party Supplier Diligence

The Company acknowledges the potential AML risk posed by contracting or outsourcing certain functions to third parties. Therefore, due diligence is conducted to establish the corporate credentials of potential partners before entering into any service agreements relevant to this Policy.

This diligence includes securing the following documentation:

- Certificate of Incorporation and Memorandum & Articles of Association
- Identification of Directors and, for private companies, shareholders
- Declaration of Beneficial Ownership
- KYC information for signatories

Additionally, third-party suppliers providing payment or processing services must submit a copy of their AML/CFT policies and procedures. These documents will be reviewed by the Compliance Officer/MLRO and the Legal team to ensure the supplier's KYC processes and AML risk management are satisfactory, considering the nature and extent of potential AML risk.

8– WIDER ENVIRONMENT

8.1 General

The Company operates an online gaming enterprise, offering its services worldwide, with the exception of the United States and Canada. The successful laundering of funds requires obfuscating the origin of illicit funds. In the Company's case, there is no

opportunity for anonymous transactions. The origin and ultimate destination of funds (in the case of winnings) are traceable to a financial instrument in the customer's name, presenting a significant obstacle for money launderers or terrorist financiers.

8.2– Market Changes

The Company provides customers with the means to bet on sports, play poker, and engage in casino gaming. The Company will comply with any changes and updates mandated by various jurisdictions. It will consult with the Legal department to implement any necessary measures required to uphold these regulations.

9 - CONCLUSION

This Policy ensures that funds are transferred only to the original financial instrument in the name of the account holder used to fund the account. When this option is unavailable, funds are disbursed via a method that can only be cashed by the named account holder.

Positive verification of the customer is conducted prior to accepting a deposit and always prior to initiating a withdrawal. Consequently, the process of deposits and withdrawals presents minimal opportunities for customers to launder funds.

Jazz Business Solution B.V.'s operations are intended for recreational gamblers, not for professional gamblers. While the potential for money laundering exists, it is adequately monitored and considered low risk. All transactions are logged, suspicious activities are investigated, and all customers, regardless of deposit amounts, are verified.

Know Your Customer (KYC) Policy

1. Purpose of this Policy

We are committed to maintaining the highest standards of integrity, security, and compliance with applicable laws and regulations. This Know Your Customer (KYC) Policy explains how we verify the identity of our players and why this process is essential for ensuring a safe and transparent gaming environment.

Our KYC procedures are fully aligned with the requirements set by the Curaçao Gaming Authority (CGA) and other applicable regulations related to Anti-Money Laundering (AML) and the prevention of fraud.

2. Scope

This policy applies to:

- All players registering on our platform;
- All transactions carried out through our services; and
- Any person or entity interacting with us in relation to our gaming activities.

By using our services, you agree to comply with this policy and to provide the information requested during the verification process.

3. Why KYC is Required

KYC procedures are implemented to:

- Verify your identity and ensure you are of legal age to participate in gaming activities;
- Prevent fraud, money laundering, and other unlawful activities;
- Protect your account and funds; and
- Comply with international regulatory obligations under the CGA framework.

These measures are designed to safeguard both our players and our platform.

4. Information We Collect

To verify your identity, we may request the following:

- **Personal Identification:** A valid government-issued document (e.g., passport, ID card, or driver's license).
- **Proof of Address:** A recent utility bill, bank statement, or official correspondence showing your name and residential address (issued within the last 3 months).
- **Payment Method Verification:** Documentation confirming ownership of the payment method used (e.g., copy of card or crypto wallet confirmation).

All documents must be clear, valid, and submitted through our secure channels.

5. Verification Process

1. **Registration Review** – Upon creating an account, you may be required to upload documents to confirm your identity.
2. **Document Authentication** – Our compliance team verifies the authenticity of the information provided.
3. **Additional Checks** – In some cases, we may request further information or documentation to complete the verification.
4. **Account Approval** – Once verification is successful, you will be able to fully access our services.

Failure to provide the requested documents may result in account suspension or closure.

6. Ongoing Monitoring

KYC is not a one-time process. We may:

- Request updated documents periodically;
- Review transactions to ensure they are consistent with your profile;
- Apply additional checks if suspicious activity is detected.

This continuous monitoring ensures compliance with CGA regulations.

7. Data Protection

All personal data collected during the KYC process is handled in strict compliance with applicable data protection laws and our Privacy Policy.

- Information is stored securely and only accessible to authorized personnel.
- We do not disclose your data to third parties unless required by law or regulatory obligations.

8. Player Responsibilities

As a player, you must:

- Provide accurate, complete, and truthful information during registration and verification;
- Update us promptly if your personal information changes;
- Cooperate with any requests for additional information or documentation.

Providing false or misleading information may lead to account termination and legal consequences.

9. Non-Compliance

Failure to comply with this policy or refusal to provide required documentation may result in:

- Account suspension or permanent closure;
- Withholding of funds until verification is completed;
- Reporting to relevant authorities, where applicable.

10. Contact Us

For any questions regarding this policy or the KYC process, please contact our Compliance Team at: compliance@isppro.net

Player Complaints Policy

1. What Is a Complaint?

A complaint is a written expression of dissatisfaction regarding any aspect of our service, decisions, or conduct. This includes issues related to deposits, withdrawals, bonuses, KYC, account restrictions, responsible gaming, data protection, or any other matter.

2. Timeframe to Submit a Complaint

You may file a complaint free of charge within 6 months of the incident or the settlement of the wager related to your concern.

For in-running sports betting, we recommend submitting your complaint promptly, as data required to assess the case may not be retained for long.

3. How to Submit a Complaint

To file a complaint:

1. Contact our Customer Support via email or live chat.

2. Required information:

- Full name and country of residence
- Account number
- Date of the complaint and the event in question
- Description of the issue
- Any relevant supporting documents

4. How We Handle Complaints

Responsible Gaming Complaints:

- Prioritized and resolved within 5 business days when possible.
- Acknowledge receipt within 2 days with details of the process and estimated timeline.

- Extensions (max 2 weeks) may apply in complex cases, or if we await further input from you.

All Other Complaints:

- Acknowledge receipt within 7 days.
- Resolution provided within 4 weeks.
- A one-time extension (up to 4 more weeks) may apply, with prior written notice.

You will receive a final written decision, including:

- A clear explanation and evidence (if applicable), or
- The reason for rejection, and
- Information on how to escalate the matter.

5. Escalation – Alternative Dispute Resolution (ADR)

If you are not satisfied with our final response, you may escalate (optional) your complaint free of charge to an independent ADR provider certified by the CGA.

- You cannot reopen a case with a different ADR once one has been chosen.
- ADR outcomes are binding for us. Some limitations may apply for repeated or very low value claims.

Contact details for our ADR provider:

The Curacao Gaming Authority (CGA) has not yet published the official list of certified ADR providers. Once the list becomes available, Jazz Business Solutions will enter into an agreement with at least one certified ADR provider and update this section with the provider's name, website, and contact information.

6. Record Keeping and Reporting

- All complaints and disputes are logged and reviewed.
- Reports are submitted to the CGA twice a year.

- We retain complaint records for up to five years, or as required by data protection and legal standards.

7. Your Legal Rights

- Nothing in this policy limits your right to take legal action.
- You may also report regulatory violations directly to the CGA.
- Note: the CGA does not mediate individual disputes but may act on misconduct or regulatory breaches.

8. Overview of Issues Covered

You can file a complaint about, but not limited to:

- Deposit or withdrawal delays
- Bonus terms and conditions
- Account suspension or closure
- Responsible gaming and self-exclusion
- KYC/Verification or data privacy concerns
- Technical or software failures
- Alleged fraud or breach of terms
- Licensing and compliance matters

9. Contact Us

If you have a complaint or require help submitting one, please contact us at:

Email: compliance@ispupro.net

Live Chat: click on the respective icon on the URL page

Security Policy

This Security Policy is addressed directly to you, the player, to explain your responsibilities and what measures we take to protect you and the integrity of our platform. While we implement stringent security measures based on Curaçao law (LOK) and best practices from regulated jurisdictions, we cannot assume responsibility for losses or breaches caused by your own errors or negligence.

1. Account and Password Security

- You are required to use strong, unique passwords on our platform; they must be at least 8 characters and include uppercase/lowercase letters, numbers. Passwords must not match your username.
- Accounts are locked after multiple failed login attempts, and sessions auto-terminate after periods of inactivity.

Your responsibility: Do not share your credentials and use secure devices and networks to access your account.

2. Data Protection and Privacy

- All personal and financial data are stored and transmitted securely, often in encrypted formats.
- We comply with applicable privacy and data-protection laws.

Your responsibility: Keep your email and profile up to date. Notify us immediately of any unauthorized access or suspicious activity.

3. Platform Security and Infrastructure

- We maintain system logs, conduct regular vulnerability assessments firewalls both online and internal system, with 24/7 monitoring Network Operations, protected by fortinet and cloudflare
- We aim for “security by design”, ensuring that our infrastructure and applications adhere to best practice technical standards protected by fortinet and cloudflare.

Your responsibility: Do not attempt to circumvent system limitations or exploit vulnerabilities; it may lead to suspension or termination.

4. Incident Reporting and Response

- We follow a formal incident escalation process. From a breach affecting player confidentiality or any service outage exceeding 12 hours, we will report the incident to Curaçao authorities in accordance with regulatory obligations.

Your responsibility: Promptly report any suspected security incident, account breach, or suspicious transaction.

5. Secure Crypto Operations

- All crypto deposits and withdrawals are monitored using blockchain analytics and transaction monitoring to detect suspicious behavior or compliance violations.

- Wallet screening prevents use of addresses associated with sanctioned entities, mixers, or darknet activity. Risk and Fraud team manage and inspect all

transactions and all transactions are blockchain protected.

Your responsibility: Only transact using wallets you control. Do not attempt to use wallets flagged or linked to high-risk services.

6. Ongoing Monitoring and Audits

- Our security protocols are reviewed periodically, and independent audit firms examine our system, controls, and compliance with AML/CFT, privacy, and security obligations.

- Our System goes through penetration tests twice per year, and we have certified cyber security personnel inhouse to maintain securely the system.

Your responsibility: Cooperate with verification requests related to audits or compliance checks as needed.

7. Disclaimer s Limitation of Liability

- Internal systems and hosting is maintained via 2FA protections for teams and secure SSL VPN.
- However, we are not liable for losses arising from:
 - o Compromised private keys or shared credentials
 - o Phishing, social engineering, or fraudulent schemes
 - o Using insecure devices or networks
 - o Your actions or misuse of the platform

Your responsibility: Implement your own personal wallet and device security practices diligently. We provide services, not individual security education.

Responsible Gaming Policy

1. Your Safety and Our Commitment

We recognize that gambling is a form of entertainment that should be enjoyed responsibly and safely. We are committed to protecting our players and fostering a secure gaming environment by implementing comprehensive Responsible Gaming measures, which include:

- Enforcing strict age verification procedures to protect individuals under 18 years of age.
- Providing players with effective tools to monitor and control their gaming behavior.
- Offering clear, accessible information and resources to promote responsible gambling.
- Continuously monitoring player behavior to identify signs of potential gambling problems and intervening appropriately when necessary.

2. Age Verification and Eligibility

Participation in gambling activities is strictly prohibited for persons under 18 years of age. Upon registration, players must confirm their age and submit valid government-issued identification for verification purposes. Should it be determined that a player is underage, we will immediately terminate the account, refund any deposits made, and cancel any winnings accrued.

3. Responsible Gaming Tools

To empower our players to manage their gaming activities responsibly, we provide the following tools accessible at all times via the Responsible Gaming section of our platform:

- **Deposit Limits:** Players may set daily, weekly, or monthly deposit caps to control expenditure.
- **Reality Checks:** Optional alerts that notify players of the duration of their gaming sessions.

- **Cooling-Off Periods:** Temporary breaks from gambling, ranging from 24 hours up to 3 months.
- **Self-Exclusion:** Options for temporary or permanent account suspension, from one year up to a lifetime, with no marketing communications during the exclusion period.

4. Self-Assessment Tools

Players uncertain about their gambling habits can access self-assessment tests available on our website. These tools assist in evaluating whether an individual may be at risk of developing problematic gambling behavior.

5. Identification of Problem Gambling

We proactively monitor player activity for indicators of potential gambling-related harm, including but not limited to:

- Frequent or excessive deposits and withdrawals.
- Cancellation of withdrawal requests.
- Prolonged or irregular gaming sessions.
- Repeated changes to gaming limits or frequent use of Responsible Gaming tools.

If such patterns are detected, we may initiate contact with the player to recommend protective measures or activate appropriate safeguards.

6. Account Suspension and Breaks

Players may opt to take a break from gambling as follows:

- **Cooling-Off Period:** Selected by the player for a duration between 24 hours and 3 months; the account remains active but with restricted access.
- **Self-Exclusion:** Full suspension of account access for a period of one year or more; reactivation requires a formal written request after the exclusion period concludes.

During any suspension period, players will not receive marketing materials or promotional offers.

7. Advertising and Marketing Practices

We are committed to ethical marketing standards. Our advertising:

- Does not target minors or vulnerable individuals.
- Does not portray gambling as a solution to financial difficulties.
- Includes clear terms and conditions alongside messages promoting responsible gaming.

8. Support Services and Resources

In addition to internal measures, we provide players with direct access to external professional support organizations, including:

- Gamblers Anonymous: www.gamblersanonymous.org
- GamCare: www.gamcare.org.uk
- GambleAware: www.begambleaware.org

9. Policy Review and Oversight

This Responsible Gaming Policy is reviewed annually to ensure ongoing effectiveness and regulatory compliance. Any significant updates will be communicated transparently to our players.

A dedicated Responsible Gaming Officer is appointed to oversee policy implementation and maintain open communication regarding responsible gaming initiatives.