

POLICY FOR THE PREVENTION OF MONEY LAUNDERING,
TERRORISM FINANCING, AND THE PROLIFERATION OF
WEAPONS OF MASS DESTRUCTION
A M L / C F T

2025

KEY INFORMATION

Title	Policy for the Prevention of Money Laundering, Terrorism Financing, and the Proliferation of Weapons of Mass Destruction
Reference Number	PL_LD_FT_SUPERJOGOS_2025
Version	V.03
Status	Valid
Approving official	Fernando Valvassori de Almeida and Isabela Mendonça <i>(Administrator responsible for policy approval and Compliance Officer), e-Management N.V., director of SPJ</i>
Responsible office	Integrity and Compliance
Effective date	February 1, 2025
Next review date:	February 1, 2026
Company	SUPERJOGOS N.V.
Keywords	Money laundering, crime, prevention, politically exposed person, terrorism, unlawful acts and counteraction; know your customer, know your employee, know your partner.



POLICY STATEMENT

This Policy sets forth the foundational principles governing compliance and risk monitoring related to Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and the Prevention of the Proliferation of Weapons of Mass Destruction (PF) at SUPERJOGOS N.V. (“[SPJ](#)”).

The purpose of this Policy is to ensure that [SPJ](#) is not utilized as a conduit for financial crimes, and to guarantee full adherence to applicable legal and regulatory requirements. It also mandates the implementation of internal measures in line with best practices to mitigate the risks associated with illicit financial activities.

This document outlines the statutory obligations applicable to financial crime prevention to which [SPJ](#) must conform, along with internal procedures adopted for compliance purposes. It shall be referred to as the Anti-Money Laundering, Counter-Terrorist Financing, and Proliferation Financing Policy (“Policy”).

SCOPE AND APPLICABILITY

This Policy applies to all platforms operated by [SPJ](#), as well as to its employees, officers, directors, managers, shareholders, suppliers, partners, and clients.

This Policy shall be subject to periodic review to ensure its continued relevance and alignment with prevailing legal and regulatory standards and shall be updated at least annually. Any amendment must be approved by the Administrator and the Integrity and Compliance Directorate.

EFFECTIVE TERM

This Policy shall remain in effect for an indefinite term and shall be reviewed and approved as specified above at least once annually, or upon any legislative change or business practice evolution that warrants its revision.

The review process shall encompass a reassessment of all risk factors addressed in this Policy, including but not limited to: user risk profiles, enterprise risk exposure (including business model and geographic scope), operations, products and services, as well as the activities

carried out by employees, partners, and outsourced service providers.

LEGISLATION

This Policy is grounded in the following legal frameworks:

- article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 n. 92) and;
- article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 n.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- NOIS;
- NORUT;
- Sanction National Ordinance;
- CFATF;
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015 (N.G. 2015 n. 30)
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

DEFINITIONS

In general, Money Laundering is defined as the set of actions aimed at concealing the true origin of funds obtained through illicit means, so that such funds appear to be legitimate. Money laundering occurs in three stages:

- (i) placement;
- (ii) layering; and (iii) integration.

Money laundering encompasses various situations related to financial crimes, such as:

- Attempts to transform illegally obtained funds into “clean” assets;
- Possession or transfer of proceeds acquired through criminal offenses such as theft and fraud;
- Possession or transfer of stolen property;
- Involvement with criminal or terrorist organizations;
- Collusion to facilitate money laundering in cooperation with criminal or terrorist groups.

There are two main modalities of money laundering within the gambling sector:

- The conversion of money, assets, goods, and properties obtained through criminal activity into legitimate and clean resources, through transfers or lawful commercial transactions; and
- The use of funds derived from criminal activities to finance gambling as a form of leisure.

Another form of misuse of resources is Terrorist Financing, in which—regardless of the origin of the funds—they are used to finance criminal acts. Terrorist Financing does not necessarily involve funds obtained through illicit means, but often seeks to obscure the origin or intended use of the resources, which will subsequently be employed in criminal activities.

Terrorist Financing refers to the raising or collecting of funds, directly or indirectly, intended to be used in terrorist acts.

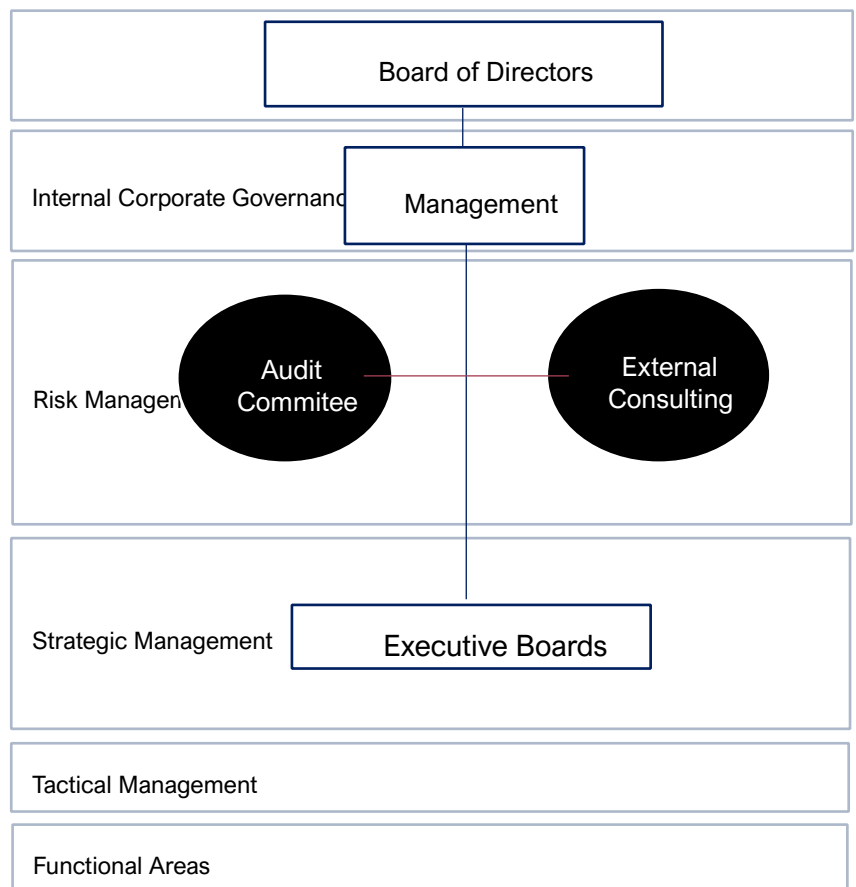
In addition, there is Proliferation Financing, which refers to the provision of funds or financial services for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, or storage of weapons of mass destruction (WMD), including chemical, nuclear, or biological weapons. This also includes the delivery of dual-use goods and technologies for illegitimate purposes, in violation of national laws or, where applicable, international obligations.

To address such acts, sanctions are imposed—these are political and economic measures adopted as part of diplomatic efforts by countries, multilateral or regional organizations, against States or organizations. These sanctions aim to protect national security interests, uphold international law, and combat threats to international peace and security.

Term	Definition
------	------------

Analyst	Person or persons designated to act on behalf of the AML/CFT Compliance Officer.
Compliance Officer	Company executive responsible for overseeing all activities related to Anti-Money Laundering (AML) and Counter-Terrorist and Proliferation Financing (CFT/CPF).
Partner	Client with whom SPJ has a direct business relationship and to whom it provides payment services.
AML	Anti-Money Laundering.
CFT	Counter-Terrorist Financing and Counter-Proliferation Financing.
CPF	Counter-Proliferation Financing.
KYC	<i>Know your client</i>
KYE	<i>Know your employee</i>
KYP	<i>Know your partner</i>
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
PEP	Politically Exposed Persons
TR	Transaction Report
SWIFT	<u>Society for Worldwide Interbank Financial Telecommunication.</u>
OFAC	<i>Office of Foreign Assets Control</i>
GAFI/FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network.
EU	European Union
UN	United Nations
UNSC	United Nations Security Council.
RBA	<i>Risk-based approach</i>
UTR	Unusual Transaction Report.
IRA	Internal Risk Assessment – A tool used to identify and analyze potential company risks to support the development of the AML/CFT framework.

METHODOLOGY



GOVERNANCE

BRANDS	Sports Betting and Online Gaming
LEGAL, RISK, AND REGULATORY	Legal and Corporate Governance; regulatory oversight (including responsible gaming); regulatory adherence; reputation and integrity care; segment-specific risk assessment; anti-bribery and anti-corruption measures; regulatory compliance and licensing; responsible gaming protocols.
CULTURE, PEOPLE, AND BENEFITS	Salary and benefits policy; operational structure of human resources; workforce strategy; management; productivity and engagement; inclusion and organizational ethics; talent recruitment and retention.
STRUCTURAL GOVERNANCE AND INTERNAL CONTROL	Corporate Governance
TECHNOLOGY	Technology infrastructure; global operational structure; technological initiatives; cybersecurity measures.
STRATEGY	Corporate Strategy



RESPONSIBILITIES



Senior management has a fundamental responsibility to lead and actively support the prevention of money laundering, financing of terrorism, and the proliferation of weapons of mass destruction by ensuring the effective implementation of policies, proper allocation of resources, and promotion of an organizational culture that emphasizes compliance and integrity in all operations.



Compliance

Set of procedures and rules aimed at keeping the organization in compliance with current standards, whether they are legal or internal.



Employees' responsibilities

- Employees are trained to follow Company' policies and procedures for customer due diligence.
- Employees must report to the MLRO any knowledge or suspicion of money laundering whether by customers, guests or other employees by drafting an internal STR.

TRANSACTIONS

The relevant department is responsible for monitoring all transactions to and from SPJ and verifying the identity of all online registered players. Company' senior management, as well as all employees and service providers, are fully committed to adopting a riskbased approach to anti-money laundering ("AML") with effort focused where it is most needed to be able to process payment transactions between the Company and customers of www.supremabet.com in a way free of money laundering issues.

The developed internal systems and procedures applied by SPJ are appropriate for remote gaming businesses like www.supremabet.com. The Company appreciates that its money laundering and terrorist financing risk assessment is not a one-off exercise, and these are assessed regularly so that adopted approach is effective at any time.

SENIORMANAGEMENT

Senior management is fully engaged in the processes around Company' assessment of risks for

- being the internal point of contact for the unusual transaction reports ("UTRs");
- reviewing and investigating STRs and considering whether a unusual activity report ("SAR") should be submitted to the authorities.

money laundering and terrorist financing and are involved at every level of the decision making to develop the appropriate policies and processes to comply with relevant legislation.

Based on this, Senior Management will appoint one of its senior officers and/or a service provider specialized in AML as the designated Money Laundering Reporting Officer ("MLRO"), whose responsibilities will include the duties required by the laws regulations and guidance notes.

MONEY LAUNDERING REPORTING OFFICER

The MLRO is responsible for the oversight of all aspects of the AML activities within the company and has the authority to act independently in carrying out his responsibilities having access to sufficient resources to carry out his duties.

All instances of suspected Money Laundering attempts must be reported to the MLRO and his duties and responsibilities include:

- identifying money laundering and terrorist financing risks relevant to the Company;
- designing and implementing policies and procedures relating to AML and countering terrorist financing ("CTF"), monitoring the effectiveness of these and reviewing and updating these policies and procedures;
- reporting to Senior Management on AML and CTF activity and the effectiveness of the Company's controls;
- keeping AML/CTF records;
- receiving internal disclosures and deciding whether these should be reported;
- training employees to ensure that they are aware of the Company's AML policies and procedures and how to report unusual transactions;

Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

Where any AML tasks are delegated within the business, the MLRO will remain responsible for all AML issues. Any delegated tasks will be

recorded and will be counter-signed by the delegate to confirm acceptance of responsibility. Employees who need to be aware of the delegation will be notified immediately.

BUSINESS RISK ASSESSMENT (BRA)

The Company shall maintain a documented Business Risk Assessment (BRA) framework to evaluate its exposure to money laundering (ML), terrorism financing (TF), and proliferation financing (PF) risks. The BRA considers at a minimum the following categories:

- Types of customers (e.g., retail players, VIPs)
- Products and services offered (e.g., online games, payment methods)
- Delivery channels (e.g., remote onboarding, affiliates)
- Geographic exposure (e.g., player location, payment providers)
- Third-party and outsourcing relationships

The BRA shall be reviewed annually or upon material changes to the Company's business model. The results of the BRA shall inform the Company's risk appetite, internal controls, customer due diligence procedures, and overall AML/CFT/CPF program. The Compliance Officer is responsible for coordinating the BRA and presenting its conclusions to Senior Management and the Board.

RESTRICTIVELISTS

To effectively manage our risk and comply with regulatory requirements and sanctions lists, all clients and partners are verified against UN sanctions and the OFAC sanctions, INTERPOL, EU Sanctions List, FATF (Financial Action Task Force), PEPs (Politically Exposed Persons) Lists, among other lists.

The Compliance Officer must, on a semi-annual basis, review the list of users registered in the [SPJ](#) system to identify potential customers or beneficiaries listed in Restrictive Lists, such as the "UN Sanctions Committee" list and the OFAC list.

The information compiled by the AML/CFT Compliance Director must be treated with absolute confidentiality. In the event of identifying customers included in the list, their registration will not be approved, and the AML/CFT Compliance Director must report all collected data to FIU.

The mere presence of a customer, user, and/or beneficiary on the "UN Sanctions Committee" list or the OFAC list is sufficient grounds to report an operation to FIU, irrespective of their involvement in any Unusual Operations.

Sanctions restrictive lists will be updated with the same frequency as this Policy, which is every 2 (two) years.

KYC – KNOW YOUR CUSTOMER

SPJ adopts the "Know Your Customer" ("KYC") procedure to help combat the threats of money laundering and other fraud across its brands.

To open an account with SPJ, the Customer must first complete the initial registration process and undergo identity verification by cross-checking the provided data with the Brazilian Federal Revenue database, collecting evidence to confirm the query.

During the "Identification Process," the Customer registers by providing information such as name, country of residence, Tax Identification Number, and phone contact. These details are verified by specialized software, which also checks additional data such as the date of birth and Tax Identification Number validity to validate the user's age and legal capacity.

Identity verification shall be conducted through the submission of documents and information, including:

- Full name;
- Date of birth;
- Place of birth;
- Nationality;
- Permanent residential address;
- Parentage and related persons;
- Full residential address;
- Tax Identification Number;
- Telephone number;
- Email address;
- Valid and government-issued identification document (e.g., driver's license, passport, or professional ID);
- Photograph of the user holding the submitted identification document beside their face; ➤ Proof of income; ➤ Proof of life.

Players must be at least 18 years old. Minors cannot complete registration on the platforms. The Company is committed to preventing underage access and will take all necessary steps to ensure they do not register on the gaming site.

After registration, the Customer receives an SMS to validate their mobile number for communication purposes. Without this confirmation, the Customer cannot complete registration.

CUSTOMER RISK ASSESSMENT (CRA)

Each player undergoes a Customer Risk Assessment (CRA) at the point of onboarding. This CRA evaluates the player's risk profile based on factors such as geography, transaction behavior, payment method, and customer type (e.g., VIP). The risk profile determines the level of due diligence and the frequency of monitoring applied.

CUSTOMER ACCEPTANCE POLICY (CAP)

Based on the Customer Risk Assessment, a Customer Acceptance Policy (CAP) is applied. This policy defines the acceptance criteria for onboarding and maintaining business relationships. Players flagged as PEPs, from high-risk jurisdictions, or presenting red flags are subject to Enhanced Due Diligence or may be rejected entirely in line with internal risk tolerance. Sanctions screening is mandatory for all players and must be passed before activation

Upon the player's first deposit on any SPJ platform, additional documents are required to verify their identity: (i) a copy of a valid personal ID; (ii) a selfie holding the ID; (iii) a recent proof of address (issued within the last 3 months); (iv) facial recognition (proof of life).

For withdrawals between €1,800.00 – €9,000.00 (BRL 10,000.01 and BRL 49,999.99), further validation is required. In addition to previous validations, income proof, bank statements from the past three months, and/or the current year's income tax return must be submitted. For withdrawals over €9,000.00 (BRL 50,000.00), all transactions are subject to manual review by the Game Security department, and approval depends on a detailed analysis of the customer's financial profile.

In such cases, the Customer must access the "Settings" > "Documents" section and provide additional documents, such as: (i) recent proof of address (issued within the last 3 months); (ii) proof of address in the name of a third party, along with proof of relationship (e.g., parent, spouse).

For deposits over €9,000.00 (BRL 50,000.00), the Customer will undergo detailed verification to prove the source of funds and will be screened against restricted lists and subject to Compliance Officer approval.

For withdrawals, basic validation will be performed for transactions up to €126.00 (BRL 700.00). For amounts above this limit and up to €900.00 (BRL 5,000.00), proof of address (issued within 3 months) and a selfie holding a valid ID will be required.

The above limits do not apply to Unusual Transactions, including:

- Financial activity inconsistent with the customer's income or profile;
- Structuring transactions to avoid monitoring limits ("smurfing");
- Frequent, high-value transfers or withdrawals without clear justification;
- Involvement of individuals or entities linked to sanctioned or high-corruption risk countries;
- Incomplete, false, or inconsistent registration information;
- Use of third-party identification to open accounts;
- Frequent changes to registration details without reasonable justification;
- Large deposits followed by immediate withdrawals without gaming activity;
- Deposits using multiple payment methods;
- High initial deposits in newly created accounts with no activity history;
- Players consistently winning or losing large sums in seemingly intentional patterns;
- Sudden changes in betting patterns, such as sharp increases in bet amounts without reason;
- Bets placed in obscure or illiquid markets;
- Excessive use of bonuses or promotions to move significant funds;
- Financial activity from sectors known for high money laundering risk;
- Attempts to withdraw to third-party bank accounts;
- Customer accounts with unusually high transaction volumes;
- Numerous small transactions over a short period to achieve high total volumes;
- Repetitive transaction patterns indicating an organized network of linked accounts;
- Transactions simulating legitimate outcomes to justify illicit fund flows.

If there are signs of money laundering, the Integrity and Compliance Department is responsible for promptly reporting.

Records of both procedures will be kept for ten years from the end of the business relationship or the customer's last platform activity.

KYC renewal is required 12 months after the initial registration or in specific situations such as unusual transactions or deposit variations above 50%.

If the "Verification Procedure" cannot be completed for any reason, the Customer will not be allowed to access their user account or withdraw any funds until documentation is regularized.

In addition, based on FATF (Financial Action Task Force) recommendations regarding Customer Due Diligence (CDD), SPJ will:

- (i) Identify the customer and verify their identity through reliable, independent documents, information, or data;
- (ii) Identify the beneficial owner and take reasonable steps to verify their identity to ensure the institution knows who the ultimate beneficiary is. For legal persons and entities, financial institutions must also understand the ownership and control structure of the customer;
- (iii) Understand and, when appropriate, obtain information about the purpose and intended nature of the business relationship;
- (iv) Conduct ongoing due diligence and scrutinize transactions throughout the relationship to ensure consistency with the institution's knowledge of the customer, their business, and risk profile, including the origin of funds when necessary.

Besides verifying the Customer through legal documents and independent sources, the Player's profile is monitored by the Security team based on their risk profile:

- Betting history;
- Game types and preferences;
- Transaction timings;
- Interactions with customer support;
- Use of bonuses and incentive programs;
 - Deposit history;
- Submitted documents;
- Types and categories of documents submitted;
- Document submission dates;
- Account details;
 - Player ID.

Although the engagement of third parties for the performance of due diligence procedures is permissible under specific conditions, SPJ elects to conduct the entirety of the Customer Due Diligence (CDD) process internally and exclusively through its own resources.

This entails that:

- i. No portion of the verification, identification, or client analysis process is outsourced, delegated, or entrusted to independent third parties, whether by contract, agreement, or any other outsourcing arrangement; and
- ii. All data collection, identity verification, risk assessment, Politically Exposed Person (PEP) determination, and ongoing monitoring of the business relationship are conducted directly by internal specialized teams under the supervision of the compliance department;

Any client onboarding, document analysis, or risk-based decision-making is within the sole and exclusive competence of the institution, and any form of outsourcing or reliance on third parties for such purposes is strictly prohibited.

Even in scenarios involving group-affiliated entities or related agents, the activities carried out by them are deemed direct extensions of the internal operation and are therefore fully subject to the same Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policies, controls, measures, and procedures adopted by the platform.

By maintaining an entirely internal process, we ensure enhanced control, standardization, and traceability of all actions related to due diligence.

PROHIBITED ACCOUNTS

The Company shall not accept or maintain business relationships with the following:

- Individuals under the age of 18
- Anonymous or fictitious account holders
- Accounts using third-party or false identities
- Customers on sanctions lists (UN, EU, OFAC, etc.)
- Persons linked to known criminal organizations
- Self-excluded individuals under Responsible Gaming rules
- Customers whose identity or source of funds cannot be verified

Any such account shall be suspended, and where appropriate, an Unusual Transaction Report (UTR) shall be submitted to FIU Curaçao.

ENHANCED DUE DILIGENCE (“ EDD ”)

Under the Regulations, there are three circumstances in which EDD on Customers should be carried out, which goes beyond identifying them and verifying their identity. These are:

- when the customer is not present, which is relevant to an online operation (this would only be relevant for the online operation);
- when the customer is a PEP;
- in any other situation where the customer presents a higher risk of money laundering or terrorist financing (e.g. a high spending customer).

In relation to Customers not being present (online operations) the requirement for additional due diligence is met by the Customer making every financial transaction only to or from a bank account in his name.

In relation to PEPs and other customers that present a higher risk of money laundering or terrorist financing, Company may seek to obtain evidence of the Customer's source of funds as follows:

- Identification documents provided by the Customer;
- Information provided by the Customer in conversation;
- Verification of identity using an online provider;
- Third party acuity and wealth reports;
- Credit reports;
- Information available in the media and on the internet;
- Search of PEP databases;
- Company registration searches for companies the customer appears to be a shareholder or officer of; □ Sanctions list.

REQUIREMENTS PROCEDURES

In the light of the requirements imposed by law and regulations, Company adopts the following procedures when Verification Procedure is triggered under the threshold approach:

- at the point that verification is triggered, Company will suspend any transaction from the User Account and no withdrawals can be made;
- further deposits can be made to that account as long as they too are locked into it until the Verification Procedure is completed;
- bets can be made from the account, again providing any winnings will remain locked until the Verification Procedure is completed;
- once the Verification Procedure is completed, the account can be unlocked and business can continue as normal;
- if the Verification Procedure cannot be completed, then Company will terminate the business relationship with the Customer;
- if there are monies to be repaid, the amount repaid will consist of the monies owed to the Customer at the point that the Verification Procedure was triggered plus all deposits made at that point and

thereafter; □ money will be returned to the originating account; □ there will be appropriate risk mitigation.

Company will use a mix of sources, including external sources and information taken directly from the customer, for EDD purposes.

ONGOING MONITORING

Monitoring customer and partners activity is carried out using the risk-based approach, with higher risk Customers, such as PEPs, being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than is appropriate for lower risk Customers. Monitoring of customers is done by the relevant employees who monitor customer activity live.

SUPPORTING RECORDS

The website www.supremabet.com will, by the nature of their business, generate detailed records of all transactions with each customer and for purposes of the record keeping requirements Company retains the drop/win figures for each named customer.

TRAINING

All relevant employees of Company are given training on AML and CTF, both at induction and by way of refresher training on an annual basis. Company ensures that employees understand the Regulations and apply the Company's policies and procedures, including the requirements for CDD, record keeping and STRs/SARs.

The MLRO, nominated officers and employees responsible for completing CDD checks are regularly given training in how to recognize and deal with transactions and other activities which may be related to money laundering or terrorist financing.

REPORTING

Under the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is legally required to detect, evaluate, and report any **unusual transaction** to the **Financial Intelligence Unit Curaçao (FIU Curaçao)** without delay.

A transaction is considered "unusual" if it matches predefined **objective indicators** or if, in the Company's judgment, it raises concern for money laundering, terrorism financing, or proliferation financing — known as **subjective indicators**

Any UTRs are considered by the MLRO, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing. Where appropriate, the MLRO will make a UTR to the FIU.

REPORTING PROCEDURE TO THE FIU

The Company is obligated under the **National Ordinance on the Reporting of Unusual Transactions (NORUT)** to report any transaction or attempted transaction that appears unusual, as defined by **objective** or **subjective indicators** issued by **FIU Curaçao**.

Monitoring and Detection

The Security Team is primarily responsible for monitoring player behavior, supervising onboarding processes, and overseeing transaction activity through automated systems and manual reviews. Their role is to identify any conduct or transactional pattern that may be indicative of money laundering, terrorism financing, or proliferation financing.

Unusual activity may be identified based on a range of objective and subjective indicators, including but not limited to:

- Financial activity inconsistent with a customer's known profile;
- Use of multiple accounts or intermediaries without clear justification;
- Frequent high-value transactions or withdrawals without economic rationale;
- Structuring of transactions (e.g., "smurfing") to avoid detection;
- Refusal to provide requested identification or supporting documentation;
- Links to Politically Exposed Persons (PEPs), sanctioned individuals or entities, or high-risk jurisdictions;
- False or inconsistent registration information;
- Third-party involvement in payments or withdrawals;
- Immediate withdrawal of large deposits without gameplay;
- Transactions involving virtual assets or industries with high ML risk;
- Unusual betting behavior, sudden changes in play patterns, or high initial deposits in new accounts;
- Evidence of account networks used for fund layering or disguise.

These and other risk factors may trigger an internal escalation for further investigation.

Reporting Indicators

The Company is obligated under the National Ordinance on the Reporting of Unusual Transactions (NORUT) to report any transaction or attempted transaction that appears unusual, as defined by objective or subjective indicators issued by FIU Curaçao.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000.00 or more;

- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as “objective indicators”, while (d) is referred to as “subjective indicator”. While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

Internal Reporting Process

When a member of the Security Team identifies potentially unusual activity, they must **formally escalate** the case to the Compliance Department within 24 hours of detection.

Upon receiving the report, a compliance analyst will:

- Conduct a full review of the customer’s account and transaction history;
- Assess the presence and relevance of risk indicators;
- Gather relevant documentation and contextual information;
- Determine whether the transaction(s) meets the legal threshold for reporting under Curaçao law.

If the analyst believes there is sufficient basis to proceed, the case is escalated to the Compliance Officer (MLRO).

External Reporting to FIU Curaçao

The Compliance Officer has the responsibility and authority to determine whether the transaction or activity must be reported to FIU Curaçao.

If the threshold is met:

- A Unusual Transaction Report (UTR) must be submitted to FIU Curaçao within 48 hours of the original detection of the activity.
- The UTR is filed electronically via the FIU Curaçao secure reporting platform.
- The report must include:
 - Full customer identification details;
 - Transaction data;
 - Description of the unusual activity;
 - Rationale for the suspicion; and
 - Supporting documentation.

Internal governance processes (e.g., review by a Compliance Committee) may be used to support case documentation but must not delay submission of the UTR. The 48-hour statutory window takes precedence.

Confidentiality and Non-Disclosure

The customer involved in the reported activity must never be informed that a UTR has been or may be filed. This is strictly prohibited under the tipping off provisions of Curaçao AML legislation.

Recordkeeping and Follow-Up

The Compliance Officer must retain all documentation related to the UTR, including internal reports, analysis, FIU filing confirmations, and correspondence. These records must be securely stored for at least 5 years, in line with applicable retention requirements.

The customer account in question shall be subject to enhanced monitoring for at least 12 months following the filing of a UTR. All actions taken must be logged and auditable

INDEPENDENT AUDIT FUNCTION

The Company shall implement an independent audit function to periodically evaluate the effectiveness of its AML/CFT/CPF framework. This function may be performed by an internal team or qualified external party and shall:

- Review policy implementation and effectiveness
- Identify control gaps and propose improvements
- Assess compliance with Curaçao AML legislation
- Report findings to Senior Management and the Board

Audit reviews shall occur at least annually, or as directed by the Curaçao Gaming Authority (CGA) or FIU Curaçao.

The results of each audit shall be documented in a written report and presented to the Compliance Officer and Senior Management. Identified weaknesses must be addressed through a documented remediation plan. The Compliance Officer is responsible for ensuring that all findings are escalated to the Board, where necessary, in accordance with the governance framework.

EXAMINATION BY THE CGA

The Company shall cooperate fully with all compliance inspections and audits conducted by the Curaçao Gaming Authority (CGA) or the Financial Intelligence Unit Curaçao (FIU Curaçao). This includes providing access to:

- Internal AML/CFT/CPF policies
- Customer and transaction records
- Reports of unusual transactions
- Evidence of training and monitoring

The Company shall act on recommendations or remediation measures issued by these regulators promptly and transparently.

COLLUSION AND CHEATING

Company has systems to detect cheating, collusion, or any illegal activity, including unusual and large transaction alerts, risk management solutions to monitor customer transaction and online risk solutions. Where unusual activity is identified, the customer's account will be reviewed, and this will be reported as an UTR to the MLRO. The Customer's account will be suspended and where cheating/collusion is identified, the account will be closed and the customer will be reported, where it is deemed necessary.

If an employee is implicated in any cheating, collusion, or other illegal activity, they will be suspended pending a full investigation.



PROTECTION OF EQUIPMENT

Company ensures that its equipment and business is protected from crime and criminal misuses by:

- keeping its premises fully locked when no member of staff is present;
- members of staff access the office by using an in-out log. This will allow tracking of staff members in case of illegal activity;
- computer equipment is protected by user-log out and password protected screensavers whenever it is left unattended, or outside office hours;
- the office premises are kept secure.

For the proper qualification of the partner and partner on the SPJ, 05 (five) main points:

- General information of the merchant:
- Copy of the certificate of registration in the corresponding Public Registry;
- Tax identification number;
- Copy of Articles of Association and Articles of Incorporation;
- Identification of the business owners or stakeholders (IDs or passports), meaning a copy of passport and proof of address for all persons who own or control, either directly or indirectly, 25% or more of the shareholding in your company;
- simple copy of the passport of the directors, representatives, administrators, legal

- representatives and authorized signatories of your company;
- If applicable, powers or authorization of legal.

Information about the business:

- Registration or license that enables the company's business.
- AML/CFT Policy;
- Business Continuity Policy;
- Data Privacy Policy;
- Compliance Policy;
- Cybersecurity Policy;
- Internal Controls Policy;
- Risk Assessment Policy

KNOW YOUR PARTNER

SPJ will implement a full “Know Your Partner” (“KYP”) policy.

For the purposes of this Know Your Partner (KYP) assessment, Partners shall include all technology service providers, storage, processing, activity management, marketing companies, as well as payment processors, AML query processors, and device confirmation messaging dispatchers. SPJ applies KYP to ensure that its Partners maintain integrity in their processes and to verify the regularity of their activities, with the aim of mitigating any procedural risks that may adversely affect players.

Here are the principles governing the relationship between SPJ and its Partners:

- (i) Transparency: We value transparency in all our client relationships, believing it to be a quality that should flow both

ways. We demand transparency from our clients as well. We believe this is one of the methods by which we build effective relationships, mitigating risks arising from their initiation and maintenance.

- (ii) Integrity and Ethics: Our relationships are initiated and conducted with integrity. We do not tolerate deviations from conduct or behaviors that are unlawful or unethical. Nor do we allow these behaviors to be adopted by our Clients, especially when they operate through our products and services.

- (iii) Risk Management: Relationships with Clients adhere to our risk management framework, which involves the assessment of processes, establishment of principles and minimum practices to be observed, and risk measurement. We do not tolerate excessive risks that harm the company structurally and always seek the best mitigators for identified risks.

In addition to requiring specific Principles, the business model also demands the application of

the KYP framework from a distinct perspective: ensuring that the Partner's processes regarding our Client are evaluated, and the existence of any Risks is detected prior to the commencement of the relationship.

SPJ also considers that the moment to conduct the KYP procedure is also the stage at which the analysis of the client's adherence to the principles described above should take place.

KYP follows a cyclical structure, where processes are not performed only once (at admission) but rather continuously. It remains structured according to the diagram below, which outlines its phases detailed in the subsequent item:

A) PROPOSAL

The processes encompassed by the practice known as KYP begin with the proposal, whether formalized or not, regarding the intention to establish a relationship with SPJ. Also referred to as Due Diligence, at this stage, information is gathered about the client, allowing for an understanding of at least:

- (i) The corporate structure and composition of the potential Partner, as well as its own ultimate beneficiaries;
- (ii) The purpose of initiating the commercial relationship;
- (iii) The existence of any impediments to the continuation of the partnership related to the Legal Entity or the individual beneficiaries of the company.

B) RISK ASSESSMENT

Upon receipt of the basic information about the intended relationship, the compliance department evaluates it, considering:

- (i) Whether the corporate information, such as the corporate structure, form of constitution, representation, and

corporate purpose, align with the purpose of the relationship;

- (ii) Whether there are any prior or contemporaneous facts regarding the company or its partners that may indicate the occurrence of excessive risks to SPJ

The assessment precedes the measurement of Risks, which occurs based on their extent and impact on SPJ. The information is submitted to the Compliance Committee, which deliberates on whether to agree or not to the commencement of the relationship.

Risks of very high nature concerning clients are considered intolerable – these are defined as events whose occurrence is almost certain and whose impact extends to generate extremely serious effects on SPJ.

C) RISK MITIGATION OR COMPENSATION

In the event that risks associated with the Partner are detected in the previous stage, which may not necessarily result in the discontinuation of the commercial relationship, the report addressed to the Committee proposes applicable controls to mitigate or compensate for uncertainties. Once deliberated, the proposal is forwarded to the partner or handled internally if the action is to be taken exclusively by SPJ. This is an essential step for the continuation of the KYP process.

D) ADMISSION

The admission of the partner is the formal process through which the business relationship commences and the partner is accepted.

Formalization takes place through the signing of a service contract. It is considered essential to have a legal and formalized relationship established through a contract with legal objects and parties.

E) MONITORING OF THE PARTNERSHIP

Periodic and regular assessments are conducted to evaluate whether the partner's corporate structure and the information provided in the proposal phase, remain valid and intact, thereby continuing to substantiate the commercial relationship.

If, by any chance, SPJ notices significant changes in the information, it may, at its sole discretion, either terminate the commercial relationship or initiate a new due diligence process.

F) OPERATIONAL MONITORING

Operational Monitoring is defined as the continuous activities carried out by SPJ to ensure, continuously, that the services and products offered are being properly utilized by the Service Beneficiaries. This is how SPJ establishes a sustainable system to contain the risks associated with its partners, transcending the admission stage and

assuming continuous responsibility for observing facts intrinsic to the relationship with the Partner.

The main objective here is to ensure, in addition to correcting any defects in the provision of services to its Clients, that the possibilities of Fraud, Money Laundering, and Financing of Terrorism are being mitigated by a continuous system.

DUE DILIGENCE - KYP

The initial Due Diligence comprises the process of preliminary verification of the company's data and its shareholders, preceding the commencement of any relationship. This involves the analysis of publicly available information on the internet, consultations with specialized private databases, and/or direct requests to Partners. The initial phase will be conducted by the Compliance department in conjunction with the contracting department.

The following documents may be requested:

- Completion of the Know Your Partner (KYP) Form by the Partner;
- Last amendment of the articles of association/bylaws, as well as the act that elected the last administration. For companies not incorporated in Brazil, the Certificate of Incorporation (COI) should be provided; Memorandum and Articles of Association; Appointment form of the first director(s); Certificate(s) of shares; Directors' Register; Members' Register;
- Copies of the administrator's personal documents. In the case of a proxy, the personal documents of the proxy should be provided;
- Copy of the company's CNPJ card and its branches, if any;
- Copies of Policies relevant to the matter of the relationship with the Partner;
- Identification of the name and contact details of authorized persons to speak on behalf of the Partner.
- The Compliance department reserves the right to request other documents not listed in this policy, as the Partner's line of business may require the presentation of other documents such as licenses, concessions, and regulatory clearances.

Similarly, depending on the sensitivity of the services provided by the partner, due diligence may seek to confirm and demonstrate the good practices and policies it adopts in its relationship with its members, based on the following behaviors:

- Good practices related to Consumer Law;
- Good tax practices and environmental practices;
- Handling of user data;

- ➡ Compliance with trademark and patent rules with the relevant authorities to avoid trademark violations;
- ➡ Presentation and provision of documentation supporting the operation;
- ➡ Fiscal and Corporate Regularity;
- ➡ Documentation regularity of its employees, partners, consultants, administrators, directors, shareholders, and all individuals involved in the operation;
- ➡ Regular compliance with legal requirements;
- ➡ Data protection, privacy, and information security;
- ➡ Organization of the company's personnel structure;
- ➡ Financial control, managerial reports, and projections;
- ➡ Consistent compliance with all legal operations, defining all necessary legal authorities, licenses, and controls to support the business continuously.

AFFILIATE PROGRAM

As part of its business model, the Company engages with third-party partners through an Affiliate Program. Affiliates refer players to the Company's platform in exchange for commission or revenue share. While affiliates do not directly handle player funds, they pose potential AML/CFT/CPF risks and must be subject to a structured Know Your Partner procedure, below:

1. Due Diligence on Affiliates

Prior to establishing a business relationship with an affiliate, the Company shall conduct appropriate due diligence to verify the identity and integrity of the affiliate entity or individual. This process includes:

- Verification of legal incorporation and business registration documents
- Identification of Ultimate Beneficial Owners (UBOs)
- Confirmation of physical address and contact details
- Screening against international sanctions lists, including UN, EU, OFAC, and local lists
- Assessment of the affiliate's business model, source of funds, and risk profile
- Confirmation that the affiliate does not operate from or target high-risk jurisdictions

Affiliates that pose a higher ML/TF risk shall be subject to Enhanced Due Diligence (EDD), including additional documentation and closer ongoing monitoring.

2. Contractual Obligations

All affiliate contracts shall include specific AML/CFT/CPF clauses, including the obligation to:

- Comply with the Company's AML policies and procedures
- Refrain from targeting jurisdictions or user segments prohibited by the Company
- Maintain accurate records of referred players and marketing activities
- Cooperate with the Company in the event of an internal or regulatory investigation

The Company reserves the right to terminate any affiliate relationship if AML/CFT/CPF risks arise or the affiliate breaches any compliance-related obligations.

3. Ongoing Monitoring and Reviews

The Company shall monitor affiliate behavior and performance on a continuous basis. This includes:

- Periodic reassessment of risk exposure
- Review of marketing content and campaigns
- Trigger-based reviews (e.g., suspicious traffic spikes, large player volumes from high-risk geographies)

The Compliance Officer may require re-verification of KYP documentation at any time and shall ensure that all affiliate partners remain compliant with Curaçao AML/CFT/CPF requirements.

KNOW YOUR EMPLOYEE

SPJ will implement a full “Know Your Employee” (“KYE”) policy.

For the proper qualification of the partner and partner on the SPJ, 05 (five) main points:

SPJ implements measures to ensure that, in its selection processes, it hires employees with good social conduct and ethics, free from any indications or evidence of involvement in money laundering and terrorism financing.

- General information and corporate matters of the company;
 - Civil, family, bankruptcy, tax executions and criminal;
 - Labor;
 - Negative media verification.
- To achieve this goal, the departments responsible for employee recruitment and management at SPJ implement the following measures, among others:
- Promotion of a culture of preventing money laundering and terrorism financing among employees.
 - Implementation of controls aimed at preventing money laundering and terrorism financing throughout the selection and hiring processes, as well as during the entire duration of the employment contract, with the goal of preventing and detecting any flaws in systems or negligent/irregular actions.
 - Implementation of measures to ensure that all employees receive ongoing training on the requirements derived from both internal and external regulations regarding the prevention of money laundering and terrorism financing.
 - Collection, verification, validation, and periodic updating of mandatory registration information for employees in accordance with internal and external regulations regarding the prevention of money laundering and terrorism financing. The updating of this information will occur at least once per year.

AML / CFTRISK POLICY

Decisions founded on understanding and evaluating risks are essential for propelling our business forward and readying it for the future. A strong focus on managing risks effectively enhances performance and financial results, safeguards both our workforce and brand integrity, and reinforces our commitment to fostering a sustainable and adaptable enterprise. Our team dedicated to risk management empowers individuals to make informed choices that foster growth and ensure commercial prosperity. We achieve this through:

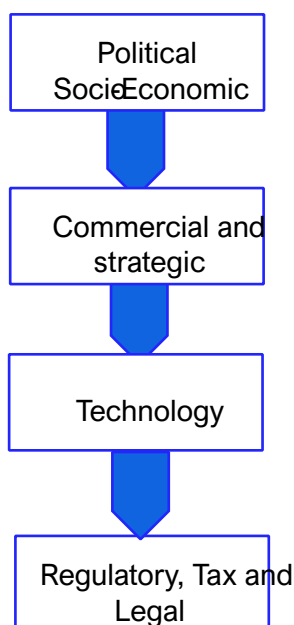
- helping people consider what might affect successful outcomes;
- balancing the pros and cons of actions and decisions;
- identifying and avoiding risks early;
- speeding up, not slowing down decision making; and
- partnering, empowering and defending the business.

The framework we've implemented spans across every division within the Group, guaranteeing a uniform and coordinated method for recognizing, handling, and communicating risks. It sets forth a structured and dependable approach to addressing both threats and opportunities across all facets of our operations. Our risk management framework is further fortified by interconnected processes that leverage the combined insights and data from SPJ' operations.

The advancement of our risk frameworks has enabled us to merge our bottom-up and top-down risk assessments, ensuring a clear understanding of threats, opportunities, and controls within the framework of both individual and collective strategic goals.

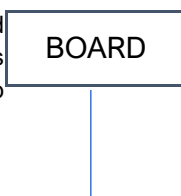
We have established a robust process for gathering perspectives on emerging risks, informed by the areas, relevant corporate subject matter experts and leadership, to provide a view of SPJ.

We define an emerging risk as a potentially significant threat with an uncertain impact that constrains our ability to confidently define a strategy and develop resources to significantly influence the materiality of the risk. Examples include technological advances, fraud complexity and legislative changes.



RISK GOVERNANCE STRUCTURE

The Board oversees the Group's internal control and risk management processes, ensuring robust systems are in place to identify, manage, and mitigate risks to the overall viability of the Group.



ETHICS AND CONDUCT EXECUTIVE COMPLIANCE AND RISK COMMITTEE AUDIT COMMITTEE COMMITTEE

The Ethics and Conduct Committee is responsible for developing, monitoring, and enforcing ethical standards and codes of conduct within an organization, ensuring compliance and fostering a culture of integrity.

The Executive Compliance and Risk Committee is a governing body within an organization responsible for overseeing and managing compliance-related matters and risks, ensuring adherence to regulatory requirements and promoting a culture of risk awareness and mitigation.

The Audit Committee has responsibility for ensuring the integrity of the Group's financial reporting and internal control and risk management systems, as well as reviewing the work of the Internal Audit function and considering the reports presented by the external auditor. On an annual basis, the Audit Committee performs an effectiveness review of the risk framework.

EXECUTIVE COMMITTEE

Day-to-day management of the business and delegated

operations. Execution of the strategy is

to the Chief Executive Officer and the Executive Committee.

First line with responsibility for: □ - ensuring ethical conduct by developing policies

□ - providing guidance, monitoring compliance, evaluating risks, and promoting a culture of integrity;

□ - create and enforce ethical standards, educate employees, investigate misconduct, assess risks, and foster an environment where ethical behavior is valued and upheld.

□ Comprising a representative from the compliance team, a representative from the human resources department, a representative from the customer service department, and a representative from the new business division.

Second line

□ risk ownership: know their businesses, know their processes and hence know their risks; □ decision making driven by risk/ reward trade-offs;

□ establishing and developing

□ the divisional risk and control

□ environment;

□ managing risk events and decisions within appetite; and □ identifying and quantifying risks.

□ Our Group functions including Group Legal & Commercial, Group Technology, Group Finance and Group People reinforce and complement the divisional second lines, and provide further

Third line Group Internal Audit team with responsibility for:

□ providing independent challenge and assurance that risks are appropriately managed;

□ systematic evaluation and monitoring of controls including internal control framework and operational effectiveness of controls; and

identifying efficiencies and process improvement opportunities.

advisory, assurance and oversight capabilities.

RISK MANAGEMENT PROCESSES

Considering the ever-changing landscape of risk and the nimbleness of our enterprise, our improved framework functions as an integral business process across all tiers of SPJ. Its alignment with strategy and performance, coupled with continuous risk management practices, will guarantee a resilient and efficient risk management system, facilitating the optimization of our brands, divisions, and the entire Group's performance.



1. **IDENTIFY** Our methodology identifies material and emerging risks.
2. **ASSESS AND QUANTIFY RISKS** Analyse risks and controls and evaluate the commercial, strategic, regulatory and other impacts, as well as the likelihood of occurrence.
3. **MITIGATE** Risk owners assess effectiveness and adequacy of controls. If additional mitigation is required, these are identified and actions plans detailed with responsibilities assigned.
4. **MONITOR AND REPORT** Management is responsible for monitoring controls and progress of actions to manage principal risks and is supported through the Group's internal audit and assurance programs which evaluate the design and effectiveness of controls.
5. **REVIEW** The risk management process is continuous and evolving

BUSINESS RISK ASSESSMENT

As part of SPJ' Compliance Program, a structured and ongoing assessment is conducted to identify and mitigate the specific risks of money laundering and terrorist financing associated with the business.

This risk assessment takes into account, among other factors:

- The types of products and services offered (e.g., sports betting, online games);
- The payment channels used for deposits and withdrawals;
- The geographic location of users;
- The behavioral and transactional profile of the customers;
- The frequency and volume of transactions.

The results of this assessment are documented, reviewed periodically, and used to adapt internal controls, preventive measures, and customer due diligence procedures.

RISK - BASED APPROACH

A Risk-Based Approach (RBA) is used, it can be established both on the basis of objective criteria and subjective criteria. Each criteria is assigned a "risk rating":

C L A S S I F I C A T I O N R E V I S I O N P E R I O D I C		
L	LOW RISK	Every 2 years*
M	MEDIUM RISK	Every 2 years*
H	HIGH RISK	Every 1 year*
FR	FORBIDDEN	N/A

*Independently of the risk certification, it will always be revised that occurs an event capable of changing the risk assessment.

The classification of each client and user will be based on at least the following criteria:

- Volume of withdrawals and deposits in the last 30 (thirty) consecutive days.
- Volume of withdrawals and deposits in the last 90 (ninety) consecutive days.
- Affirmative declaration of PEP.
- Verification of administrative and judicial proceedings involving financial crimes.
- Negative Media.
- Omission of Information:
 - Failure to provide required documentation.
 - Omission to verify telephone numbers. - Omission of proof of address.

The Company, as part of its AML Program, conducts a risk analysis to identify specific criteria for possible money laundering risks. This risk-based approach includes identifying the money laundering and terrorist financing risks (to the extent that such a risk can be identified) of clients and partners, categories of clients and volume of play that enable the Company to determine and apply proportionate measures and controls to mitigate these risks. Although the risk assessment is routinely carried out at the beginning of the client relationship, for some clients the full risk profile may only become apparent when the customer starts playing games, making deposits and withdrawals on the platform. Therefore, monitoring customer transactions and ongoing reviews are essential components of the company's risk-based approach.

In addition, this type of risk assessment process can also be adjusted for a specific customer based on information received from a competent authority. The Company assesses money laundering and terrorist financing risks using categories that provide a strategy for managing potential risks, enabling the Company to subject clients to proportionate controls and supervision.

The weight given to these risk categories (individually or in combination) in assessing the overall money laundering risk may vary according to the specific circumstances of the company.

COUNTRY OR GEOGRAPHIC RISK

SPJ services are not provided to players located in the countries listed below: Uganda, Iraq, South Africa, Croatia, Slovenia, Greece, Sweden, Romania, Belarus, Switzerland, Lithuania, Monaco, Estonia, Latvia, Isle of Man, Afghanistan, Antigua and Barbuda, Australia, Austria, Belgium, Bulgaria, Cayman Islands, Cuba, Cyprus, Czech Republic, Denmark, Kingdom of the Netherlands (Netherlands, Curaçao, Aruba, Bonaire, Sint Maarten, Sint Eustatius, Saba), France, French Guiana, French Polynesia, French Southern Territories, Guadeloupe, Germany, Hong Kong, Hungary, Iran, Ireland, Israel, Italy, Japan, Kahnawake, Libya, Macao, Malta, Martinique, Mayotte, Myanmar, Netherlands, Netherlands Antilles, North Korea, Philippines, Poland, Portugal, Reunion, Russia, Saudi Arabia, Serbia, Singapore, Slovakia, Spain, Sudan, Syria, Turkey, United Kingdom, United States of America, Vatican City, Yemen, Ontario, Canada.

Additionally, we do not render services to players who:

- Are professional players in any sport, competition, or league where SPJ offers betting;
- Are restricted by limited legal capacity;
- Are acting on behalf of another party;
- Are classified as compulsive problem gamblers, and/or are included (whether voluntarily or involuntarily) on any register or database of excluded players;
- Are depositing funds originating from criminal and/or other illegal activities;
- Are depositing funds through a Card which the Account Holder is not authorized to use and/or utilizing a Card in a jurisdiction where betting and gaming are prohibited;

- Are conducting criminal activities whereby a SPJ Account is directly or indirectly involved;
- Are using the Services in a manner that is illegal in their country of residence or otherwise restricted for them to open a gaming account, purchase or use services from SPJ, and/or otherwise participate in the games offered. It is the Account Holder's responsibility to ensure their use of SPJ Website and Services is legal;
- Find the Website or the Services offensive, objectionable, unfair, or indecent.

All players are required to keep their registration up to date, including their first and last name, country of residence, valid e-mail address and telephone number.

Country risk, together with other risk factors, provides useful information on potential money laundering and terrorist financing risks. Factors that may result in a country being determined to be at higher risk include: Countries subject to sanctions, embargoes, or similar measures issued by the United Nations ("UN") as an example. In addition, some circumstances that subject countries to sanctions or measures similar to those issued by organizations such as the UN, but which may not be universally recognized, may receive credit from the Company due to the position of the issuer and the nature of the measures.

Countries that, according to reliable sources, lack laws, regulations, and other adequate measures to combat money laundering. The term "reliable sources" refers to information prepared by organizations recognized that enjoy a general reputation and that make such information generally available to the public.

Sources can be supranational or international organizations such as the International Labor Organization (ILO), International Monetary Fund (FMI), the World Bank, and the Egmont Group of Financial Intelligence Units, as well as relevant national government agencies and non-governmental organizations. The information provided by these reliable sources does not have the effect of a law or regulation and should not be considered an automatic determination that something is of increased risk.

The risk associated with countries and geographical areas, SPJ considers the risk related to:

- a) The jurisdictions in which the client and beneficial owner are based;
- b) The jurisdictions of the main centers of activity of the client and beneficial owner; and
- c) The jurisdictions with which the client and beneficial owner have relevant personal ties.

The company defines a list of jurisdictions with which it does not cooperate, as well as a list of high-risk countries based on the FATF high-risk jurisdictions with which and other monitored jurisdictions, the programs of US and UE sanctions. The Company uses a combination of sources to identify high-risk jurisdictions, including:

- The Financial Action Task Force (FATF) "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring"
- The Curaçao Gaming Authority's published list of high-risk jurisdictions
- Internal assessments conducted as part of the BRA process

SANCTIONS AND FREEZING OF FUNDS

SJP's performs regular checks against national and international sanctions lists, including those issued by the United Nations (UN), European Union (EU), Financial Action Task Force (FATF), and the Office of Foreign Assets Control (OFAC).

If a positive match is identified with any individual or entity on such lists, the following actions will be taken:

- Immediate freezing of all funds associated with the account;
- Suspension of all active transactions;
- Prompt reporting to the competent authority, in accordance with applicable law.

These procedures are a critical component of **SPJ**' compliance framework and are regularly reviewed to ensure alignment with evolving legal and regulatory requirements.

RISK MITIGATION STRATEGIES

The company has implemented the following risk mitigation strategies:

Customer identification, due diligence, and KYC procedure. The company has implemented a KYC Program that allows staff to form a reasonable belief that they know the true identity of each merchant and the types of business and transactions that are involved in. In general, this program:

1. Promptly identifies and verifies the identity of each client;
2. Takes reasonable risk-based measures to identify and verify the identity of any beneficial owner;
3. Obtains appropriate additional information to understand the client's circumstances and activity, including the anticipated nature and level of transactions;
4. Evaluates risks that the client may pose taking into account appropriate risk variables before making a final determination. This due diligence process includes:
 - 4.1. A standard level of due diligence that is applied to all clients when entering into or continuing a relationship, such as (example):
 - 4.1.1. Identification of high-risk geographic areas, including clients located in areas of high risk of money laundering and related financial crimes, or carrying out business operations in such areas.
 - 4.1.2. Persons whose main source of funds comes from a salary, pension, social benefits from an identified and appropriate source and whose transactions are proportional to the funds.
 5. The standard level is increased concerning clients who are considered higher risk due to their location or if they hold or have held any public office, which may require greater supervision. This includes individuals who typically commit fraud against online gaming platforms or have any involvement in game outcomes, especially in sports betting.
 - 5.1. These enhanced due diligence procedures include, among others:
 - 5.1.1. Heightened awareness among company staff regarding higher-risk clients;
 - 5.1.2. Increased levels of identity confirmation procedures and income verification.
 - 5.1.3. Escalation for player retention approval on the platform;
 - 5.1.4. Understanding the normal and expected transactions of a customer, including increased monitoring of deposits and withdrawals;
 - 5.1.5. Heightened levels of ongoing controls and frequency of relationship reviews; and
 - 5.1.6. Reporting unusual activities in accordance with applicable reporting requirements.

RECORD KEEPING

SPJ maintains detailed records of gaming operations conducted through **SPJ** for a minimum period of 10 (ten) years, which must include the following information:

- (i) type of operation (withdrawal, deposit, winnings, and losses);
- (ii) customer or user data;

- (iii) risk classification of the user profile;
- (iv) whether there was communication regarding the unusual operation.

Additionally, due diligence data will be stored for the same period, starting from the termination of the relationship with SPJ.

POLITICALLY EXPOSED PERSONS (PEP) CONTROL

The following paragraph applies to every prospective merchant that SPJ engages with, aiming to ascertain whether the client is associated with politically exposed persons.

In cases where a PEP is identified:

- Prior to establishing a course of action, approval from senior management must always be sought.
- The source of income must be determined.
- Interaction on the platform shall be subject to enhanced and continuous monitoring.

Establishing the Origin of Funds

It is imperative that, before registering a player identified as a PEP, the source of their funds is legitimate and within internally established thresholds. All user transactions will be monitored to prevent the use of funds derived from corruption (i.e., bribery), fraud, or attempts by the PEP to withdraw/conceal assets from their country of origin.

ACTION PLAN

SPJ will constantly assess the effectiveness of the policy, procedures, and internal controls.

SPJ annually develops an action plan aimed at addressing deficiencies identified through the effectiveness assessment of the AML/CFT policy.

The progress of implementing the action plan must be documented through a follow-up report. The action plan and the respective follow-up report must be submitted to the institution's board of Directors for awareness and evaluation by June 30 of the year following the base date of the AML/CFT policy effectiveness report.

RELATED COMMUNICATION

SPJ has a Whistleblowing Channel that allows external individuals and employees to report unusual circumstances of money laundering, terrorism financing, corruption, fraud, or violations of internal and external regulations while preserving the anonymity of the whistleblowers.

CONTACT INFORMATION

For any questions regarding this policy, please contact:

Compliance Officer, compliance@suprema.group

POLICY URL AND GENERAL PROVISIONS

This Policy applies to the following brands:

Brands	URL
Maxima Bet	maximabet.net
Bettt	bettt.com
Boombets	boombets.com
Ganhe	ganhe.bet
Meugreen	meugreen.com
Pegobet	pegobet.com
XP Games	xpgames.bet

It is within the competence of the Executive Board of SPJ to amend this Policy whenever necessary.

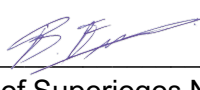
This Policy comes into effect on the date of its approval by the Executive Board and revokes any documents to the contrary.

This Policy is valid until 12/2025 unless its adaptation to endogenous and exogenous factors to SPJ that may develop during this period is deemed necessary.

Version History

Version	Reason	Date	Prepared by	Approved by
1	Initial version	February 2024	Compliance Analyst	Fernando Valvassori de Almeida, Administrator, and Isabela Mendonça, Director of Integrity and Compliance
2	First revision	February 2025	Compliance Analyst	Fernando Valvassori de Almeida, Administrator, and Isabela Mendonça, Director of Integrity and Compliance
3	Second revision (Compliance with AML/CFT in Curaçao)	July 2025	Compliance Analyst	Fernando Valvassori de Almeida, Administrator, and Isabela Mendonça, Director of Integrity and Compliance, e-Management N.V., Director of SPJ

In witness whereof, Superjogos N.V. has caused this Policy to be duly executed this 12th day of August 2025



By: e-Management N.V. as Director of Superjogos N.V.

PL_LD_FT_SUPERJOGOS_20251.v AML - final.....

Final Audit Report

2025-08-13

Created:	2025-08-12
By:	Sharella Bitoria (sharella.bitoria@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAI3A4sf-znI5-oC5hz-fLPqghbdiWXyYr

"PL_LD_FT_SUPERJOGOS_20251.v AML - final....." History

-  Document created by Sharella Bitoria (sharella.bitoria@hbmgroup.com)
2025-08-12 - 9:23:24 PM GMT
-  Document emailed to Annesol Melaria (annesol.melaria@hbmgroup.com) for signature
2025-08-12 - 9:23:29 PM GMT
-  Email viewed by Annesol Melaria (annesol.melaria@hbmgroup.com)
2025-08-13 - 7:55:38 PM GMT
-  Document e-signed by Annesol Melaria (annesol.melaria@hbmgroup.com)
Signature Date: 2025-08-13 - 7:57:13 PM GMT - Time Source: server
-  Document emailed to Bryon Finies (bryon.finies@hbmgroup.com) for signature
2025-08-13 - 7:57:14 PM GMT
-  Email viewed by Bryon Finies (bryon.finies@hbmgroup.com)
2025-08-13 - 8:31:26 PM GMT
-  Document e-signed by Bryon Finies (bryon.finies@hbmgroup.com)
Signature Date: 2025-08-13 - 8:32:04 PM GMT - Time Source: server
-  Agreement completed.
2025-08-13 - 8:32:04 PM GMT