

# Satoshi Gaming Group N.V.

## Business Overview

Satoshi Gaming Group, founded in 2019, is licensed and regulated by the Government of Curacao. <https://trustdice.win>, an online casino for crypto players, is the project operated by Satoshi Gaming Group.

## Organizational Structure

|     |            |
|-----|------------|
| CEO | Yongfu Cao |
| CCO | Yongfu Cao |

## Business Forecast

Satoshi Gaming Group is projected to generate 250,000 EUR in revenue with a future growth rate of 10%.

## Key Market Strategy

- Further develop relationships with affiliates
- Enhance our online presence by optimizing SEOs, and regularly updating our blog with relevant and informative content within the next year

# Suppliers

## Softswiss

We have built stable relationships with Softswiss as our game providers for the past 5 years.

## PG Soft

We have built stable relationships with Softswiss as our game providers for the past 5 years.

# Risk Evaluation

Satoshi Gaming Group has put in place an SGG Financial Crime Risk Assessment and Anti-Money Laundering / Counter-Terrorist Financing Policy (collectively, the "Risk and AML Policies"). The Policies are revisited periodically and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing. All senior management and employees of TrustDice are required to acknowledge and be familiar with the Policies.

# Legal and Governance

Satoshi Gaming Group has its own dedicated compliance team responsible for tracking compliance and monitoring day-to-day activities, using relevant compliance tools, making everyday activities easier to control.

# **Target KPIs and Objectives**

Satoshi Gaming Group is committed to building a trusted brand for long-term success. We strive to cultivate transparent and fair practices, establishing partnerships with reputable organizations, encouraging responsible gambling, complying with the government, and prioritizing user satisfaction and security.

## **Policies and Procedures**

1. SGG-AML Policies attached
2. SGG Financial Crime Risk Assessment attached

## SGG-AML Policies

TrustDice has put in place an Anti-Money Laundering / Counter-Terrorist Financing Policy (collectively, the “AML Policies”). The Policies are revisited periodically and amended from time to time based on prevailing industry standards and international regulations designed to facilitate the prevention of illicit activity including money laundering and terrorist financing. All senior management and employees of TrustDice are required to acknowledge and be familiar with the Policies.

This document covers AML Policies regarding TrustDice’s gaming services, which is TrustDice’s main business activity.

### Money Laundering Risks

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Terrorist financing is an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

**The risk of money laundering or terrorist financing on TrustDice is extremely low.**

TrustDice does not engage in any exchange transactions between currencies, whether in crypto or fiat. Clients can only deposit cryptocurrency (BTC) and withdraw the same cryptocurrency (BTC), with no exchange activity happening in between. TrustDice uses third party crypto transaction monitoring and source of funds software to track and tag funds deposited into its platform, making it extremely unattractive for potential bad actors attempting to move illicit funds.

All Client funds remain in “virtual” currencies and are never converted to any other currencies. TrustDice requires KYC identification documents from Clients that have deposited more than \$100 worth of currencies as an extra measure of risk reduction and compliance.

### Risk-Based Approach

TrustDice adopts and maintains a Risk-Based Approach (“RBA”) towards assessing and containing the money laundering and terrorist financing risks arising from any transactions it has with Clients. The guidelines are as follows:

- Before entering into any transaction or proposed transaction, necessary checks shall be conducted in line with the RBA so as to ensure that the identity of the Clients does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations;
- For the purpose of risk categorization of the Clients, the relevant information shall be obtained from the Clients at or before the time of entering into a transaction;
- The risk categorization process for different types of Clients may take into account the background of the Clients, country of origin, sources of funds, volume of turnover or deposits, as well as social and financial background;
- The outcome of the risk categorization process shall be decided based on the relevant information provided by the Clients at the time of commencement of business relationship;
- Enhanced due diligence would be required for higher-risk Clients, especially those for whom the sources of funds are not clear, or for transactions of higher value and frequency, which shall be determined by TrustDice at its sole and absolute discretion; and
- TrustDice must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the TrustDice in compliance with the relevant legislations in place.

TrustDice does not serve clients from certain regions that are deemed high-risk or unwelcoming from a legal or regulatory perspective, including Cuba, Iran, North Korea, Syria, and the United States of America.

### Sanctions

TrustDice does not open accounts or transact with individuals that are on prescribed sanctions lists. TrustDice screens against United Nations, European Union, UK Treasury, US Office of Foreign Assets Control (OFAC), and other sanctions lists in all jurisdictions in which TrustDice operates.

## Politically Exposed Persons

TrustDice does not open accounts or transact with individuals who are Politically Exposed Persons (PEPs), or their family members. TrustDice screens all Clients against global PEP lists before they are allowed to establish a relationship with TrustDice.

## Internal controls

TrustDice implements and maintains internal controls for the purpose of ensuring that all of its operations comply with AML legal requirements and that all required reports are made on a timely basis.

# The transaction monitoring process of SGG

TrustDice places a high priority on compliance and anti-fraud management. The risk management, finance, and customer support teams at TrustDice work together on the entire transaction monitoring process to manually halt and investigate each transaction that a customer has completed.

TrustDice diligently monitors transactions (including the tips function) for suspicious activity. All client funds remain in “virtual” currencies and are never converted to any other currencies. Transactions that are unusual are carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose.

The menu we adopted:

- SGG-Customer Onboarding/ KYC/CDD Policy
- SGG-AML Policies
- SGG-Compliance Policy

For the purpose of the Policies, a “Suspicious Transaction” means a transaction or attempted transaction, which to a person acting in good faith:

- gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- appears to be made in circumstances of unusual or unjustified complexity;
- appears to have no economic rationale or bona fide purpose; and
- gives rise to a reasonable ground of suspicion that it may involve financing activities relating to terrorism.
- consider a general bar of a single €10,000 transaction high-risk.
- For the tips function, consider a general bar of a single €100 as high-risk.

Procedure :

- Basic KYC of the customer. PEPs, blocklists, and watchlist screening. a) require to submit ID; b) then manually checks the data (if documents edited or not).
- Transaction analysis: monitoring of previous and future transactions; identification of unusually large, frequent, or uncommon transactions. GeoComply: device sharing; jumping location, IP address - whether the user has multiple accounts; betting activity: based on the user’s betting behavior.
- Sending a report to the compliance team to ask for an investigation into suspicious transactions.
- Risk assignment: The compliance team of our group will investigate and determine the risk level of a transaction based on business policy.
- Deliver an end report and keep records. Take action to close suspicious accounts according to the policy.

# SGG-Compliance Policy/Framework

## Compliance Policies Framework

The policies are designed to lay down a framework to:

- prevent TrustDice from being used, intentionally or unintentionally, by criminal elements for money laundering or financing terrorist activities;
- enable TrustDice to know and understand its customers, clientele, contributors, and other contacts with which TrustDice has any financial dealings with (collectively, "Clients") and their financial background and source of funds better, which in turn would help it to manage its risks prudently;
- put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws, procedures and regulatory guidelines; and
- equip employees and contractors of TrustDice with the necessary training and measures to deal with matters concerning KYC/AML procedures and reporting obligations.

Our Policies will be reviewed and updated on a regular basis to ensure appropriate procedures and internal controls are in place to account for both changes in regulations and changes in our business.

## Compliance Officer

The Compliance Officer is the person, duly authorized by TrustDice, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of TrustDice's anti-money laundering and counter-terrorist financing, including but not limited to:

- Collecting Clients' identification information;
- Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations;
- Monitoring transactions and investigating any significant deviations from normal activity;
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;
- Updating risk assessment regularly;
- Providing law enforcement with information as required under the applicable laws and regulations.
- The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing, and other illegal activity.

## Monitoring and Reporting

TrustDice diligently monitors transactions for suspicious activity. Transactions that are unusual are carefully reviewed to determine if it appears that they make no apparent sense or appear to be for an unlawful purpose. When such suspicious activity is detected, the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

Suspicious activity can include more than just suspected money laundering attempts. Activity may be suspicious, and TrustDice may wish to make a filing with a law enforcement authority, even if no money is lost as a result of the transaction.

The Compliance Officer initially makes the decision of whether a transaction is potentially suspicious. Once the Compliance Officer has finished his review of the transaction details, he makes the decision as to whether the transaction meets the definition of suspicious transaction or activity and whether any filings with law enforcement authorities should be made.

For the purpose of the Policies, a "Suspicious Transaction" means a transaction or attempted transaction, which to a person acting in good faith,

- gives rise to a reasonable ground of suspicion that it may involve proceeds of criminal or other illicit activity, regardless of the value involved;
- appears to be made in circumstances of unusual or unjustified complexity;
- appears to have no economic rationale or bona fide purpose; and
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Ongoing monitoring is an essential element of effective implementation. TrustDice diligently monitors transactions for Suspicious Transactions and other suspicious activity.

## **Record-keeping**

Our AML Compliance Officer is responsible for ensuring that AML records are maintained properly.

We document our verification, including all identifying information provided by a Client, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We keep records containing a description of any document that we relied on to verify a Client's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we retain documents that describe the methods and the results of any measures we took to verify the identity of a Client.

We also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We retain records of all identification information for seven years after the account has been closed, or as long as reasonably necessary to comply with applicable regulations; we retain records made about verification of the customer's identity for seven years after the record is made, or as long as reasonably necessary to comply with applicable regulations.

## **Training**

All new employees receive anti-money laundering training as part of the mandatory new-hire training program. All applicable employees are also required to complete AML and KYC training annually. Participation in additional targeted training programs is required for all employees with day-to-day AML and KYC responsibilities.

Our training includes, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags (3) what employees' roles are in TrustDice's compliance efforts and how to perform them; (4) TrustDice's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance.

Our operations are regularly reviewed to check whether certain employees require specialized additional training. Written procedures are updated to reflect any such changes.

## SGG Financial Crime Risk Assessment



This assessment is designed to prevent financial crime by meeting the UK standards on combating money laundering and terrorism financing. [Regulation 18](#) of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and the Money Laundering and Terrorist financing (amendment) regulations 2019 requires you to perform a risk assessment on your practice, in order to identify and assess the risks of money laundering and terrorist financing to which your practice is subject.

### Instruction

- Complete the assessment by considering whether the specified risks affect your practice and ticking YES or NO as appropriate.
- Should your answer identify a risk, then proceed to provide further information, and outline the risk level and action you are currently implementing or proposing to implement, to mitigate and manage the risk.
- Should a risk not be applicable, please mark the risk as N/A. Should a risk or risks affect your practice that are not identified, add these to the appropriate section and complete them in the same manner.

| AREA AND NATURE OF RISK                                                                                                                                                                                                                                                                                                                                                     | YES                      | NO                       | ACTION TO MITIGATE AND MANAGE THE RISK<br>(describe the actions you have taken, or propose to take, to mitigate the risks) | Risk Level:<br>High/Med/<br>Low |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------|
| <b>Customer Risk Factors</b>                                                                                                                                                                                                                                                                                                                                                |                          |                          |                                                                                                                            |                                 |
| 1. <b>Non face-to-face clients:</b> Does our practice have any clients or client representatives who we have not met face-to-face <sup>1</sup> ?                                                                                                                                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> | [If yes, provide information on this risk and the action taken to mitigate it]                                             | [If yes, give the risk level]   |
| 2. <b>CDD measures:</b> Does our practice obtain information from a reliable source which is independent of the person whose identity is being verified, where that process is secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity <sup>2</sup> | <input type="checkbox"/> | <input type="checkbox"/> | [If yes, provide information on this risk and the action taken to mitigate it]                                             | [If yes, give the risk level]   |
| 3. <b>Politically exposed persons (PEPs):</b> Does our practice ascertain whether clients are PEPs <sup>3</sup> ?                                                                                                                                                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | [If no, provide the remedial action you will take]                                                                         | [If no, give the risk level]    |

<sup>1</sup> This is a high-risk factor under [regulation 33\(6\)](#), which may indicate there is a high-risk of ML or TF

<sup>2</sup> [Regulation 28\(19\)](#) sets out these factors.

<sup>3</sup> The definition of a PEP includes UK, domestic and overseas persons. This includes family members and known close associates, under [regulation 35](#).

|                                                                                                                                                                                                                                                                                                                      |                          |                          |                                                                                |                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------------------------------------------------------------|-------------------------------|
| 4. <b>Locations:</b> Does our practice have any clients:<br><ul style="list-style-type: none"> <li>- From a high-risk third country as identified by the European Commission<sup>4</sup>?</li> <li>- From other high-risk countries<sup>5</sup>?</li> <li>- Connected to high-risk countries<sup>6</sup>?</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/> | [If yes, provide information on this risk and the action taken to mitigate it] | [If yes, give the risk level] |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------------------------------------------------------------|-------------------------------|

|                                                                                                                                                                                                                                                                                                                                                                      |                          |                          |                                                                                |                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------------------------------------------------------------|-------------------------------|
| <b>Products and Services</b>                                                                                                                                                                                                                                                                                                                                         |                          |                          |                                                                                |                               |
| 1. <b>Our services:</b> Does our practice provide:<br><ul style="list-style-type: none"> <li>- Services to user from high risk region<sup>7</sup>?</li> <li>- Services that involve handling or managing client money or assets?</li> </ul>                                                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> | [If yes, provide information on this risk and the action taken to mitigate it] | [If yes, give the risk level] |
| 2. <b>Our locations:</b> Does our practice operate in any online casino restricted country/ high-risk countries <sup>8</sup> ?                                                                                                                                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> | [If yes, provide information on this risk and the action taken to mitigate it] | [If yes, give the risk level] |
| 3. <b>Reliance:</b> Does our practice:<br><ul style="list-style-type: none"> <li>- Rely on another regulated person to identify and verify the identity of clients (and beneficial owners, if applicable)?</li> <li>- Use an agent or outsourcing service provider to identify and verify the identity of clients (and beneficial owners, if applicable)?</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/> | [If yes, provide information on this risk and the action taken to mitigate it] | [If yes, give the risk level] |

|                                                                                                                                                                                                                                                                                 |                          |                          |                                                    |                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|----------------------------------------------------|------------------------------|
| <b>Practice compliance</b>                                                                                                                                                                                                                                                      |                          |                          |                                                    |                              |
| 1. <b>AML/CTF policy:</b> Does our practice:<br><ul style="list-style-type: none"> <li>- Have an AML/CTF policy that reflects the money laundering legislation<sup>9</sup>?</li> <li>- (If applicable) Communicate its AML/CTF policy to all employees<sup>10</sup>?</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/> | [If no, provide the remedial action you will take] | [If no, give the risk level] |

<sup>4</sup> Business relationships with clients established in countries [identified by the European Commission as high-risk](#) are automatically high-risk business relationships under [regulation 33](#).

<sup>5</sup> [Regulation 33\(6\)](#) sets out factors to help identify such countries.

<sup>6</sup> The connection may be the client's customers, suppliers, or the countries in which it operates. [Regulation 33\(6\)](#) sets out factors to help identify such countries.

<sup>7</sup> This is a high-risk factor under [regulation 33\(6\)](#), which may indicate there is a high-risk of ML or TF

<sup>8</sup> [Regulation 33\(6\)](#) sets out factors to help identify such countries.

<sup>9</sup> A written AML/CTF policy is required that includes at least the matters set out in [Regulation 19](#). CIMA's [AML/CTF policy](#) has been updated according to the money laundering legislation.

<sup>10</sup> [Regulation 19](#) requires your AML/CTF policy, and any changes to it, to be communicated within your practice and a record maintained of the steps you took to communicate it.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                          |                          |                                                    |                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|----------------------------------------------------|------------------------------|
| <b>2. CDD and client risk assessment process:</b> Does our practice have a CDD and client risk assessment process that reflects the money laundering legislation <sup>11</sup> ?                                                                                                                                                                                                                                                                                                                                                                                       | <input type="checkbox"/> | <input type="checkbox"/> | [If no, provide the remedial action you will take] | [If no, give the risk level] |
| <b>3. Data protection and terms of engagement:</b> Do our terms of engagement include: <ul style="list-style-type: none"> <li>- Data protection information that new clients must be provided with<sup>12</sup>?</li> <li>- Obtaining client consent to hold personal information for longer than 5 years after the business relationship ends (should we wish to so hold it)<sup>13</sup>?</li> </ul>                                                                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> | [If no, provide the remedial action you will take] | [If no, give the risk level] |
| <b>4. (If applicable) Employee training:</b> Has our practice provided to all relevant employees: <ul style="list-style-type: none"> <li>- Awareness of the law relating to money laundering and terrorist financing, and to the requirements of data protection<sup>14</sup>?</li> <li>- Regular training in how to recognise and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing<sup>15</sup>?</li> <li>- A record in writing of the above awareness and training<sup>16</sup>?</li> </ul> | <input type="checkbox"/> | <input type="checkbox"/> | [If no, provide the remedial action you will take] | [If no, give the risk level] |
| <b>5. (If applicable) Two client files</b> have been reviewed to ensure they contain adequate CDD information and meet the practice's AML/CTF policy. These files were: <ul style="list-style-type: none"> <li>1) Full name, date of birth</li> <li>2) Valid ID Client holds in their hand</li> </ul> Did the files contain adequate CDD information and meet the practice's AML/CTF policy?                                                                                                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> | [If no, provide the remedial action you will take] | [If no, give the risk level] |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                          |                          |                                                    |                              |
| <b>[For risks applicable to your practice that are not covered above, add more rows as necessary to the relevant section]</b>                                                                                                                                                                                                                                                                                                                                                                                                                                          |                          |                          |                                                    |                              |
| <b>Declaration</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                          |                          |                                                    |                              |
| <b>Practice name:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |                          |                                                    |                              |
| <b>Name of the person who has completed this assessment:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                          |                          |                                                    |                              |
| <b>Name of the Money Laundering Reporting Officer (if different):</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                          |                          |                                                    |                              |
| <b>Date:</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                          |                          |                                                    |                              |

<sup>11</sup> [Regulation 28](#) requires certain information to be obtained and verified when performing CDD. [Regulation 28\(16\)](#) requires your client risk assessment to be documented and take into account at least certain factors. CIMA's [CDD templates](#) have been updated to reflect the money laundering legislation and contain client verification and risk assessment processes.

<sup>12</sup> [Regulation 41\(4\)](#) requires you to provide certain data protection information to new clients before you enter into a business relationship. Please see CIMA's [mandatory requirements page](#) for more information.

<sup>13</sup> [Regulation 40](#) requires you to delete personal data obtained for the purpose of the Regulations after 5 years from when the business relationship ended.

<sup>14</sup> [Regulation 24](#) requires such awareness to be provided.

<sup>15</sup> [Regulation 24](#) requires such training to be provided.

<sup>16</sup> [Regulation 24](#) requires such a written record to be produced and maintained.

