

Know Your Customer Policy (KYC Policy)

Customer identification and verification:

The formal identification of users/customers on entry into commercial relations is a vital element, both for the regulations relating to money laundering and for the KYC Policy.

This identification relies on the following fundamental principles:

A copy of your passport, ID card or driving license, each shown alongside a handwritten note mentioning six random generated numbers. Also, a second picture with the face of the user/customer is required. The user/customer may blur out every information, besides date of birth, nationality, gender, first name, second name and the picture. To secure their privacy.

Please note that all four corners of the ID have to be visible in the same image and all details has to be clearly readable besides the named above. We might ask for all details if necessary.

An employee may do additional checks if necessary, based on the situation.

Proof of Address:

Proof of address will be done via to different electronic checks, which use two different databases. If an electronic test fails, the user/customer has the option to make a manually proof.

A recent utility bill sent to your registered address, issued within the last 3 months or an official document made by the government that proofs your state of residence.

To make the approval process as speedy as possible, please make sure the document is sent with a clear resolution where all four corners of the document is visible, and all text is readable.

For example: An electricity bill, water bill, bank statement or any governmental post addressed to you.

An employee may do additional checks if necessary, based on the situation.

Source of funds:

If a player deposits over a five thousand euro there is a process of understandings the source of wealth (SOW).

Examples of SOW are:

Ownership of business

Employment

Inheritance

Investment

Family

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible an employee may ask for an additional document or prove.

The account will be frozen if the same user deposits either this amount in one go or multiple transactions which amount to this. An email will be sent to them manually to go through the above and an information on the website itself.

Goldeneggs.casino also asks for a bank wire/credit card to further insure the Identity of the user/customer. It also gives additional information about the financial situation of the user/customer.

Basic document for step one:

The basic document will be accessible via the setting page on Goldeneggs.casino. Every user/customer has to fill out the following information's:

Full name

Permanent residential address

Date of Birth

Place of Birth

Nationality

Identity number

Risk management:

In order to deal with the different risks and different states of wealth in different regions on the earth Goldeneggs.casino will categorize every nation in three different regions of risk.

Region one:

Low risk:

For every nation from the region one the three-step verification is done as described earlier.

Region two:

Medium risk:

For every nation from the region two the three-step verification will be done at lower deposit, withdraw and tip amounts. Step one will be done as usually. Step two will be done after depositing 1000\$ (one thousand Dollars), withdrawing 1000\$ (one thousand Dollars) or tipping another user/customer 500\$ (five hundred Dollars.) Step three will be done after depositing 2500\$ (two thousand five hundred Dollars), withdrawing 2500\$ (two thousand five hundred Dollars) or tipping another user/customer 1000\$ (one thousand Dollars). Also, users from a low risk region that change crypto currency in any other currency will be treated like user/customers from a medium risk region.

Region three:

High risk:

Regions of high risks will be banned. High risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

According to a risk based few and general experience the human employees will recheck all checks which are done before by the other employees and may redo or do additional checks according to the situation.

In addition, a data scientist supported by modern, electronic, analytic systems will look for unusual behavior. For example, attempts to use a different Bank account to for Deposit and Withdraw, nationality changes, currency changes, behavior and activity changes as well as checks, if an account is used by it's original owner.

Also a user/customer has to use the same method for Withdraw as he used for Deposit, for the amount of the initial Deposit to prevent any Money Laundering.

In any case, Goldeneggs.casino conducts a Customer Due Diligence (CDD) when users/customers make financial transactions in the amount of at least 2000\$.

Enterprise-wide risk assessment:

As part of its risk-based approach, Goldeneggs.casino has conducted an AML “Enterprise-wide risk assessment” (EWRA) to identify and understand risks specific to Goldeneggs.casino and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The users/customers to whom services are offered, transactions performed by these users/customers, delivery channels used by the bank, the geographic locations of the bank’s operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on Goldeneggs.casino understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is yearly reassessed.

All users/customers are checked against UN and EU sanctions lists:

- UN Sanctions List <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>;
- EU Sanctions List <http://www.sanctionsmap.eu/#/main>.

Ongoing transaction monitoring:

AML-Compliance ensures that an “ongoing transaction monitoring” is conducted to detect transactions which are unusual or suspicious compared to the user/customer profile.

This transaction monitoring is conducted on three levels:

1) The first Line of Control:

Goldeneggs.casino works solely with trusted Payment Service Providers whom all have effective AML policies in place as to prevent the large majority of suspicious deposits onto Goldeneggs.casino from taking place without proper execution of KYC procedures onto the potential user/customer.

2) The second Line of Control:

Goldeneggs.casino makes its network aware so that any contact with the user/customer or player or authorized representative must give rise to the exercise of due diligence on transactions on the account concerned.

In particular these include:

Requests for the execution of financial transactions on the account;

Requests in relation to means of payment or services on the account;

Also, the three-step verification with adjusted risk management should provide all necessary information’s about all costumers of Goldeneggs.casino at all time.

Also, all transaction must be overseen by employees over watched by the AML compliance officer who is over watched by the general management.

The specific transactions submitted to the customer support manager, possibly through their Compliance Manager must also be subject to due diligence.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC), their financial behaviour and the transaction counterparty.

The transactions observed on user/customer accounts for which it is difficult to gain a proper understanding of the lawful activities and origin of funds must therefore rapidly be considered atypical (as they are not directly justifiable).

Any Goldeneggs.casino staff member must inform the AML division of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known of the user/customer.

3) The third Line of Control:

As a last line of defence against AML Goldeneggs.casino will do manually checks on all suspicious and higher risk users/customers in order to fully prevent money laundering. If fraud or Money Laundering is found the authorities will be informed.

Reporting of Suspicious transactions on Goldeneggs.casino:

In its internal procedures, Goldeneggs.casino describes in precise terms, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

Reports of atypical transactions are analysed within the AML team in accordance with the precise methodology fully described in the internal procedures.

Depending on the result of this examination and on the basis of the information gathered, the AML team:
will decide whether it is necessary or not to send a report to the FIU (The Financial Intelligence Unit Curaçao), in accordance with the legal obligations provided of legislation; or
will decide whether or not it is necessary to terminate the business relations with the user/customer.

Procedures:

The AML rules, including minimum KYC standards will be translated into operational guidance or procedures that are available on the Intranet site of Goldeneggs.casino.

Record keeping:

Records of data obtained for the purpose of identification must be kept for at least five years after the business relationship has ended.

Records of all transaction data must be kept for at least five years following the carrying-out of the transactions or the end of the business relationship.

These data will be safely, encrypted stored offline and online.

Training:

Goldeneggs.casino human employees will make manual controls on a risk based approve for which they get special training.

The training and awareness program is reflected by its usage:

- A mandatory AML training program in accordance with the latest regulatory evolutions, for all in touch with finances;
- Academic AML learning sessions for all new employees.

The content of this training program has to be established in accordance with the kind of business the trainees are working for and the posts they hold. These sessions are given by an AML-specialist working in Peak Progress Partners N.V. AML team.

Auditing:

Internal audit regularly establishes missions and reports about AML activities.

Data Security:

All data given by any user/customer will be kept secure, will not be sold or given to anyone else. Only if forced by law, or to prevent money laundering data may be shared with the AML-authority of the affected state.

Goldeneggs.casino will follow all guidelines and rules of the data protection directive (officially Directive 95/46/EC).

Contact us:

If you have any questions about our KYC Policy, please contact us:

By email: support@goldeneggs.casino

If you have any complains about our KYC Policy or about the checks done on your Account and your Person, please contact us:

By email: support@goldeneggs.casino