KNOW YOUR CLIENT POLICY & ANTI MONEY LAUNDRING
(hereinafter – «Policy")

PURPOSE

Due to national and international regulations on the prevention of criminal activities and money laundering, and terrorism financing, the Company (CyberBridge OÜ, a private limited company organized under the laws of Estonia) strictly implements KYC guideline and procedure.

We respect and honor the confidentiality of our clients, corporate and individuals, nevertheless we are committed to undertake thorough due diligence of both our clients' identities and the nature of their businesses.

It is our obligation not just to undertake a full and proper due diligence of our clients' and their current needs, but also to monitor and ensure that their business activities do not breech any national and international regulations with regards to money laundering and terrorism financing.

1. This Policy of the Company is to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Company requires its officers, employees and affiliates to adhere to these standards in preventing the use of Company's Services for money laundering purposes.

2. For the purposes of this policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

3. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

4. Each employee of Company, whose duties are associated with the provision of products and services of Company and who directly or indirectly deals with Client of Company, is expected to know the requirements of the applicable laws and regulations which affect his job responsibilities, and it shall be the affirmative duty of such employee to carry out these responsibilities at all times in a manner that complies with the requirements of the relevant laws and regulations.

5. To ensure that this Policy is carried out, management of Company has established and maintains an ongoing program for the purpose of assuring compliance with the relevant laws and regulations and the prevention of money laundering. This program seeks to coordinate the specific regulatory requirements throughout the group within a consolidated framework in order to effectively manage the group's risk of exposure to money laundering and terrorist financing across all business units, functions, and legal entities.

6. Each of the Company's affiliates is required to comply with Policy.

7. All identification documentation and services records shall be kept for the minimum period of time required by local law.

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

8. Client is obliged:

8.1. to respect any requirements of law, including international, directed on fight against illegal trade, financial frauds, washing and legalization of the money received in the illegal way;

8.2. to exclude direct or indirect complicity of illegal financial activities and to any other illegal operations with use of the Company's website.

9. Client guarantees a legal origin, legal ownership and availability at Client of the actual right to use of the money transferred by Client.

10. In case of suspicious or fraudulent cash replenishments, including use of the stolen credit cards and/or any other activities of fraudulent nature (including any returns or cancellations of payments), Company reserves the right to stop provision of Services and to block Client's Account, and also to cancel results of any Operations performed by Client and to investigate operations of doubtful nature owing to what to suspend such operations before clarification of the nature of emergence of money and the end of investigation.

11. During the investigation Company reserves the right to request from Client of the copy of the identity certificate (passport) and bank cards used for account replenishment, the payment, and also other documents confirming legal possession and a legal origin of money.

12. Client is forbidden to receive and use Services and/or the software for any illegal or fraudulent action, or for any illegal or fraudulent Operations (including money laundering) according to the legislation of the country of jurisdiction of Client or Company.

13. Refusal of Company of carrying out suspicious Operations isn't the basis for any Company's civil responsibility before Client or other third parties for non-execution of any liabilities in relation to Client.

14. Clients are therefore invited to provide below listed documents to comply with our KYC policy to our partner KYC&AML-service provider, Shufti Pro company, according to the list and demands stated at: http://shuftipro.com/documents-we-verify/ http://shuftipro.com/how-it-works/ and Annex 1 hereto.

PERIODICITY

15. To ensure that the information that the Company holds on its customers is always accurate and up to date, Company shall, upon its' sole discretion, determine the periodicity at which each individual customers shall be, upon request, obliged to provide their KYC information anew to continue using Company services.

DISCLAIMER

16. Company is entitled, upon its sole discretion and grounding upon KYC&AML policy, at any time during the service provision to its clients demand them present the documents (list of which shall be constituted solely by Shufti Pro including the form of the documents to be presented) to reinstate account functionality or justify any other action (or operation) performed (or about to be performed) by the client. Such requests will be done via email.

17. Simultaneously, Company reserves the exclusive right to unilaterally decline any clients' application and/or terminate further provision of services without any statements or explanations to the client.

Annex 1

Order of KYC and AML clients' inspection

Each consequent inspection step to be fulfilled only after the completion of the previous one.

KYC - The Client should approve his or her personality through the personality identification including submission of his/her ID and visual information (face picture). The personality identity should be validated by Shufti Pro.

AML – a) the client's identity would be checked by Shufti Pro in all applicable AML databases on his or her primary approach to CyberBridge's services and b) the client's absence in the AML databases should be re-checked every 11 minutes.

Inability of the client to comply the demands of Shufti Pro on every stage of the inspection mentioned above (the inspection finds the Client inappropriate) leads to denial of services provision by the Company.

Shufti Pro procedure of KYC inspection

STEP 1

User is asked to look into the camera. It's facial recognition system will focus on key facial features and take a snapshot.

STEP 2

User is asked to display a photo ID (Driving license, Passport etc.) or credit/debit card.

STEP 3

User is asked to bring the Document close to the camera. In case credit/debit card, the first 6 digits need to be in clear display for the process to continue. In case of passport or driving license, the name should be in clear display to the camera to proceed further.

STEP 4

User is asked to display the first 6-digits and last 4-digits of the credit/debit card and in case of driving license, ID card and/or passport, the user has to display the date of birth in clear view to the camera.

Verified data

ID Card

✔ Face Detection
✔ Liveness Detection
✔ Selfie comparison with card
✔ Physical ID card Detection
✔ Name on ID card
✔ Date of Birth on ID card

Passport

✔ Face Detection
✔ Liveness Detection
✔ Selfie comparison with Passport
✔ Real Passport Detection
✔ MRZ Code Validation
✔ Name on passport verification
✔ Date of birth on passport

Driving License

✔ Face Detection
✔ Liveness Detection
✔ Selfie comparison with License

✔ Real Driving License Detection
✔ Name on DL verification
✔ Date of birth on DL

Credit/Debit Cards

✔ Face Detection
✔ Liveness Detection
✔ Real Credit/Debit card detection
✔ Name on credit/debit verification
✔ First 6 digits of card number
✔ Last 4 digits of card number