Anti-Money Laundering Policy and Customer Onboarding Protocol

I. Introduction

E-Wisestan (The "Company" or "E-Wisestan") is required and committed to comply with all law that apply to its activity.

The Company is active in the e-commerce space and is offering to and receiving solutions from various merchants, therefore money laundering and the financing of terrorism have been identified as material risks to be addressed by the Company.

As a prudent actor in the e-commerce services field, the Company will act in accordance with the industry applicable standards for prevention of money laundering and terror financing through its services.

The Company defines "compliance" as the adherence to laws and regulations, rules, market standards and internal codes of conduct in matters concerning observing proper standards of market conduct, managing conflicts of interest, and specifically dealing with matters such as the prevention of money laundering and terror financing, alleged corrupt and fraudulent behavior.

The requirements of the different legislations apply to the Company globally. The Company may have additional local policies and procedures designed to comply with their local legislation, regulations and any government approved guidance in the jurisdiction(s) in which they operate.

II. SCOPE

This Policy applies to all business activities of the Company.

This Policy applies to and will be implemented by all staff and any third party the Company might do business with.

III. WHAT THIS POLICY AIMs TO PREVENT

This Policy is indented to minimize the risk of the Company's services to be used for money laundering or terrorism financing.

MONEY LAUNDERING

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

Criminal conduct may be of various types and shapes and may include failure to pay taxes or when a party is acting without required licenses and permits.

TERRORISM FINANCING

Terrorism financing, in general, is facilitating the availability of funds or assets, by any means, directly or indirectly for the purposes of terrorism – including acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes.

Compared with money laundering (which involves the proceeds of all crimes), the amount of money that could be used as terrorism financing is relatively small and may be derived from legitimate sources.

As the Company adheres to all laws and is dealing only with legitimate activities, it cannot take part in such actions that might inadvertently support terror.

GIVEN THE SERVICES OFFERED BY THE COMPANY, FAILURE TO COMPLY WITH THIS POLICY MAY LEAD TO MATERIAL HARM TO THE COMPANY'S BUSINESS MODEL IF ITS COUNTERPARTIES CONSIDER THE COMPANY AS MATERIAL RISK FOR MONEY LAUNDERING AND TERROR FINANCING. THEREFORE IT IS PARAMOUNT FOR COMPANY BUSINESS TO MINIMIZE MONEY LAUNDERING AND TERROR FINANCING RISK.

IV. Purpose

1. Establish stages of customer on-boarding ;
2. Clearly define and allocate oversight responsibilities, ensuring monitoring and adherence to the Policy;
3. Prevent risks originating from being associated with customers who pose a risk to the Company, and where such association alone is in violation of applicable regulation, can result in harm to the Company's reputation, or any other loss.
4. Set the Company's guidelines under which the Company shall conduct Know-Your-Customer, identify and authenticate the customer, and maintain records of these actions.
5. Set out guidelines for monitoring customer's activities and assess on going risk.

V. Responsibilities and Authority

1. The Company shall appoint a Compliance Officer.
2. The Compliance Officer shall have the overall responsibility for adherence with this Policy and setting out rules and procedure that ensure compliance with the Policy.
3. All employees are individually responsible to ensure adherence to the Policy.

VI. Customer Onboarding Protocol

The Company shall comply with the following protocol for engaging with and on-boarding new customers (the "**Protocol**").

The Company shall not perform any transactions on behalf of the customer prior to the completion of the Protocol to the satisfaction of the Compliance Officer.

1. General

As a matter of principle, the Company will, at all times, as part of its ongoing KYC internal procedure, perform continuous monitoring on customers' activity and transactions, assess customer's economic profile, detect high-risk factors, transactions or customers, mark them for enhanced due diligence ("**EDD**") and report such customers where it is necessary under applicable law or regulation. This Protocol also requires the Company to become familiar with its customers, nature of their affairs, business, sources and expected activity in the accounts.

In general, customer due diligence (CDD) measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable,

independent source documents, data or information; (b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer; (c) Understanding and, as appropriate, obtaining information on the purpose and intended

nature of the business relationship, focusing on the nature of the transactions to be serviced by the Company; (d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

UBO - The beneficial owner is the natural person who ultimately owns or controls the account holder or at whose behest the business relationship is established. Control/ownership is presumed by law to exist if a person directly or indirectly controls more than 25 per cent of the shares or voting rights. Thus, a legal entity / registered company could have up to three beneficial owners.

2. Procedure

2.1. Sales department shall contact the customer, collect Basic Information (as defined below/in Annex [A]), complete the customer's application, and

ensure proper recording of all information obtained. The Basic Information/ customer application shall be submitted to Compliance department for review.

2.2. Compliance department shall verify and consider the Basic Information and determine whether to preliminarily accept or reject the customer's application.

2.3. General consideration guidelines:

Review information/documents provided for consistency, signatures where necessary

2.3.1. Information provided by customer:

Enhance Due Diligence ("**EDD**") territories –EDD territory involvement – as defined in Annex D, such as incorporation of customer entity/parent/subsidiaries, addresses, tax residence, address/citizenship of director/shareholder/UBO, substantial operations).

Restricted Territories – in addition to the EDD territories Annex D lists territories which with no business shall be conducted and customer associated with such Restricted Territories will not be on-boarded.

Unregulated/EDD business – customer has unregulated activities, customer activities are not subject to AML requirements at the source, requests for processing of EDD territory currency.

2.3.2. Independent review:

Customer website(s) - review for clearly fraudulent content.

Specific Industry standards – currency

2.3.3. If the customer's application is APPROVED, Compliance department shall notify and instruct Sales department how to proceed with KYC (Standard or EDD).

2.3.4. If the customer's application is REJECTED, Sales department shall contact the customer and advise on possible remediation options as specified by Compliance department. Upon remediation to the satisfaction of Sales department, the application shall be re-submitted to Compliance department for a second review as per section 2.2.

2.4. Sales department shall contact the customer and collect all applicable KYC documents as instructed by Compliance department (as defined below/in Annex [B]) within a reasonable time.

2.5. Compliance department shall verify and consider the KYC documents and determine whether to accept or reject the customer's application.

2.6. General consideration guidelines:

While the customers offer services in areas that are considered and riskier for money laundering activities, the customers are required to take active steps to reduce the risk.

The customer is required to present his risk mitigation measures and monitoring programs.

2.6.1. If the customer's application is APPROVED, Compliance department shall notify and instruct Sales department how to proceed with the customer.

2.6.2. If the customer's application is REJECTED, Sales department shall contact the customer and advise on possible remediation options as specified by Compliance department. Upon remediation to the satisfaction of Sales department, the application shall be re-submitted to Compliance department for a second review as per section 2.4.

2.7. Sales department will ensure proper Business Procedure / execution of Service Agreement and accompanying documents if any.

2.8. Compliance department shall provide written approval and instruct/initiate onboarding completion/Delivery Procedure.

VII. Risk assessment guidelines

One of the most important aspects of Anti-Money Laundering and Terrorist Financing (AML/CFT) compliance is analyzing, on an ongoing basis, our customers' economic profile and risk factors, and review the underlying transaction in view of the customer's risk grade provided to him based on such profile.

This responsibility requires us to monitor and identify transactions, evaluate them in real time, and flag those that are suspicious. This Section of the Procedure is aimed to assist trained employees to flag suspicious transactions as efficiently as possible and to provide means to recognize clues that a transaction's or customer's potentially risk. Customer who has an increasing number of flagged transactions will be required to undergo an EDD process as a condition for a continued engagement.

There are number of factors that may be considered to determine such risk factors, mostly concerning a customer's behavior, the list below is to provides some general "red-flags" to assist us to identify such risk factors and to identify the need for an Enhance Due Diligence (EDD).

1. Detecting Money Laundering

A suspicious transaction is a transaction which gives rise to suspicion for any reason. Where there is a business relationship, a suspicious transaction will often be the one which is inconsistent with a customer's known, legitimate business or personal activities. Therefore, the first key to recognition is knowing enough about the customer and the customer's business to recognize that a transaction, or series of transactions, are unusual. The "reasonable grounds for suspicion" test is both objective and subjective.

Some of these "red flags" are easier to spot during due diligence, while others, such as transactions patterns, value of assets, criminal records etc. may be very difficult to identify. In either case, our employees and managers are trained to recognize potential risks and put them under a magnifying lens for a closer look.

2. Grounds for Suspicion

Corporate:

Unusual structures, including offshore companies, trusts or structures in circumstances where the customer's business needs do not support such requirements may be suspicious; Formation of subsidiaries in circumstances where there appears to be no commercial reasoning or other purpose (particularly overseas subsidiaries);

Territory risk factors:

Customer is from (or incorporated in) any country or jurisdiction in relation to which the FATF has called for countermeasures or EDD measures (See Appendix D); Customer is from (or incorporated in) any country or jurisdiction known to have inadequate measures of preventing money laundering and the financing of terrorism.

Insufficient information:

AML compliance involves due diligence in the scrutiny of a customer. One of the first clues something is wrong would be that the customer provides dubious information. For example: documents that cannot be verified, multiple tax ID numbers, reluctance to provide detailed information about the business/UBO, or shielding the identity thereof.

Change in transaction patterns:

Currency transactions change in number, or volume; transaction patterns are significantly different from those for other similar businesses.

Sector related risks

Increased chargeback rates may indicate suspension activities.

Material change in transaction volume – number of transitions or value of the transactions

VIII.Document guidelines

Supportive documents provided to us by a customer must be authentic and provide a clear understanding of the parties involved. Such document should be:

Dated [make sure the agreement is valid];

Duly signed by all parties; and provide a CLEAR reference to the following:

The identity of the sender [make sure the funds are going out from sender's account];

The identity of the beneficiary (and its relationship with sender) [make sure the funds are going in the beneficiary's account];

Table of Annexes

ANNEX A – Basic Information

1. Legal name(s) of customer entity including any “brand names”, “doing business as”, “trading as” or assumed names;
2. Incorporation details for customer entity and any parents/subsidiaries (i.e. country of incorporation);
3. Registered addresses for each entity;
4. Tax residency;
5. Names and addresses for all shareholders, directors, secretary (if any are companies/entities, items 1 through 5 are required for each entity);
6. Names, addresses, for all UBOs;
7. Nature of business/source of funds cleared (Forex/Trading, Gaming, Gambling)
8. Regulated/unregulated activities
9. Which countries does the entity operate in
10. Subject to AML regulation in the country of incorporation?
11. Required processing currencies

ANNEX B – Standard KYC Document Checklist

#	Document	Approval		Comments
		Yes	No	
1	Certificate of incorporation			
2	Registration of shareholders			
3	Registration of directors			
4	Passport copies: Company shareholders/ directors			
5	Notarized passport copies: authorized signatories, UBOs			
6	Company utility bill (from last 6 months)			
7	Company website			
8	Company main contact phone and email			

9	Billing contact phone number		
10	Bank account details		
11	Perform PEP & Sanctions check on the sender: Watchlist, **And** global terror lists.		

ANNEX C – EDD KYC Document Checklist

#	Document	Approval		Comments
		Yes	No	
1	Certificate of incorporation (notarized)			
2	Registration of shareholders (notarized)			
3	Registration of directors (notarized)			

4	Notarized passport copies: shareholders/ directors		
5	Notarized passport copies: authorized signatories, UBOs		
6	Background checks: shareholders/ directors/ authorized signatories		
7	Company utility bill (from last 3 months)		
8	Company website URL		
9	Main contact phone and email		
10	Billing contact phone and email		
11	Bank account details		
12	Proof of ownership of bank account from which the payment will be made		
13	Expected single/weekly/monthly/ yearly transaction volume		
14	Expected volume of “At Risk Transactions” (EDD country source)		
15	Perform PEP & Sanctions check on the sender: Watchlist, **And** global terror lists.		

ANNEX D –

EDD TERRITORIES

1. Albania
2. Barbados
3. Botswana
4. Burkina Faso
5. Cambodia
6. Cayman Islands
7. Democratic People's Republic of Korea (DPRK)
8. Haiti
9. Iran
10. Jamaica
11. Lebanon
12. Malta
13. Mauritius
14. Morocco
15. Myanmar
16. Nicaragua
17. Pakistan
18. Panama
19. Philippines
20. Senegal
21. South Sudan
22. Syria
23. Uganda

24. Yemen

25. Zimbabwe

RESTRICTED TERRITORIES

1. United States of America
2. Israel