

META TECH INNOVATIONS B.V.

Fraud Management Procedures

14/08/2024

Table of Contents

Content	Page
Version History	3
Scope	4
Bank Accounts	4
Currency of Operation	4
Risk and Responsibilities Management	4
(a) Risks	4
(b) Responsibilities	4
Internal Fraud Management Procedures	5
(a) Fraud Prevention	5 - 7
(b) Fraud Investigation	7
External Fraud and Anti-Money Laundering and Counter Funding of Terrorism Management Procedures	7
(a) KYC (Know Your Client) / KYB (Know Your Business)	7 - 8
(b) Anti-Money Laundering and Counter Funding of Terrorism	8

Version History

Ver.	Description	Author	Date
1.0	Document Created	Danny Vincent Dass	15/08/2024

Scope

The purpose of this document is to define Meta Tech Innovations B.V. (hereinafter: “Company” or “Meta Tech Innovations B.V.”)’s procedures for preventing fraud from being carried out in or through the Company.

Bank Accounts

Meta Tech Innovations B.V. possesses one main bank account:

- Operations Account

The profit made by Meta Tech Innovations B.V. will be transferred to this account. All transaction for the operation of the business, including payment to services providers, payment of salaries and other relative expenses shall be undertaken from this account. Meta Tech Innovations B.V. intends to primarily work with Bank of Valletta (BOV) in Malta and possibly other additional banks.

Currency of Operation

The currency of operation will be Euro.

Risks and Responsibilities Management

Meta Tech Innovations B.V. will take into consideration the following risks and responsibilities in mind throughout the operation of its business:

(a) Risks

Fraud and corrupt conduct may be carried out in multiple ways. Meta Tech Innovations B.V. acknowledges that the first step to be taken in the fight against fraud and corruption shall be to establish the risks to which it is being exposed. While new risks and methods through which fraud and corruption may be carried out may arise from time to time, Meta Tech Innovations B.V. acknowledges the existence of the following:

- Misappropriation of funds;
- Fraudulent disbursements;
- Tampering with confidential information and disclosure of such to external third parties.

(b) Responsibilities

Meta Tech Innovations B.V. acknowledges that it shall be responsible to implement an effective framework of rules, policies and procedures through which it can combat fraud and corruption. The Company divides its efforts into two sectors in this scenario:

- Fraud prevention and detection; and
- Fraud Investigation.

Internal Fraud Management Procedures

(a) Fraud Prevention

Meta Tech Innovations B.V. acknowledges that it is essential to implement fraud prevention and detection procedures and policies and commits itself to direct its efforts more towards the prevention of fraud rather than on remedying post-fraud situations. In order to be able to prevent fraud, the risks to which the Company is being exposed should be clearly envisaged by the Company. For this purpose, Meta Tech Innovations B.V. shall undertake regular studies and keep itself abreast of developments which may be made in this area so as to always be up to date and informed about new and emerging risks to which it may be subject and the latest innovations in fraud prevention and detection.

The prevention framework that is being implemented by Meta Tech Innovations B.V. shall mainly comprise of the following pillars:

- Implementation of control measures and policies in order to prevent fraud;
- Adoption of surveillance and other means for the purposes of detection of fraudulent behaviour both internal and external through deception;
- Investigation of suspicious conduct or activities;
- Coherent and efficient whistle blowing policies and procedures.

Meta Tech Innovations B.V. shall implement an array of internal controls and general procedures which are to be made use of by the Company and its employees on a day-to-day basis in respect of the management and running of the daily operations of the business. Such internal controls shall mainly focus on the following principles:

- Authorisation controls

Certain actions shall require the approval or authorisation of senior management personnel prior to being able list the actions to be carried out by employees. Furthermore, a system of levels of access shall be implemented throughout the Company, whereby access to data and other inside information owned by the Company shall only be granted to selected employees. Such access and the extent to which it is granted shall be determined according to the role and position of the relevant employee. At all times, no employee shall have any access which is in excess of his needs in order to be able to perform the work which is expected of him through his role and position.

- Segregation of duties

Duties to be performed by employees shall be allocated in such a manner that no one employee shall have full and sole control over an entire process or an entire area. This prevents fraudulent behaviour from being undertaken by employees as a result of the level of power they are granted over a particular section of the operation. In cases where it would not be beneficial for the Company to have a particular duty or task split between different employees, it shall be ensured that the employee who is given full control over such process

or area shall be adequately supervised in proportion with the fraud risk level that such process or area may pose.

- Checks on performance

Senior level personnel shall carry out checks on employees on a regular basis; or whenever the need for such checks to be performed is felt by the Company. In particular, such checks shall be carried out when a suspicion arises in relation to the behaviour of specific employees. These checks may be carried out through surprise spot checks, inventory counts or other procedures which will enable such personnel to verify whether employees are complying with the policies and procedures that are in place.

- Employment Screening

Prior to engaging employees, Meta Tech Innovations B.V. shall carry out thorough searches into their integrity, among other character traits. The Company will not employ any persons who are not deemed to be fit and proper. Once a person is employed with Meta Tech Innovations B.V., screening shall still be carried out on an ongoing basis and at regular intervals so as to ensure that the integrity of such person is still intact. The frequency and extent of screening which shall be carried out shall be proportionate to the risk level posed by the employee.

- Whistle Blowing Procedures

Meta Tech Innovations B.V. shall adopt a whistle blowing procedure whereby employees within the Company may report suspicious activity, fraudulent or unethical behaviour or irregularities to particular members of senior management. All reports lodged by employees shall be treated with strict confidence. Under no circumstances shall the identity of the reporting employee be disclosed to any other employee, least of all, to the reported employee/s. Such reports shall be made to a person designated as a Fraud Prevention Officer, who shall be a member of senior staff within the Company.

Once a report is lodged by an employee, this will be treated seriously by the Company. All reports shall undergo checks and investigations in order to determine their veracity or lack thereof. Any suspicion of fraud or corruption shall be taken very seriously and will be examined and analysed with precision. Where a report is deemed to be frivolous or unwarranted, this shall also be investigated.

The results of any investigation that shall be undertaken as a result of the lodging of a report by an employee shall be laid down in a report which shall be retained by the Company. Such report shall include an explanation of the findings of the Fraud Prevention Officer that has carried out the investigation into the matter, thereby providing the reasons for which particular actions were taken or otherwise.

- Education

Meta Tech Innovations B.V. believes in the education of its employees, for which reason it shall carry out induction training sessions for each employee upon commencement of employment. Such training sessions shall be focused on fraud prevention, detection and ancillary matters. Furthermore, refresher training sessions shall be provided on a regular basis so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made thereto.

(b) Fraud Investigation

When an investigation has come to a close and has uncovered evidence of fraud or corruption, Meta Tech Innovations B.V. shall delve in depth into the facts at hand in order to establish whether the matter is of a grave enough nature to be reported to the relevant law enforcement authorities in Curacao in accordance with Curacao law. However, Meta Tech Innovations B.V. shall, regardless of whether it reports such fraudulent behaviour to the relevant authorities or not, take disciplinary action against the employee/s in question.

The company shall reserve the right to engage professional external consultants to investigate fraudulent activity.

The type of disciplinary action which shall be undertaken by the Company shall depend on the nature and extent of the fraud or corruption in question. Disciplinary action shall range from severe warnings being given to the relevant employee/s where the fraudulent or corrupt activities are not of a grievous nature to termination of employment in severe cases.

External Fraud and Anti-Money Laundering and Counter Funding of Terrorism Management Procedures

(a) KYC (Know Your Client) / KYB (Know Your Business)

Know Your Client is the due diligence carried out by the Company to identify its clients and ascertain relevant information to commence a working relationship with them. Meta Tech Innovations B.V. shall undertake to ensure that an operator is reliable and trustworthy. This shall be done by performing certain checks and studies prior to entering into a relationship with such customer. Meta Tech Innovations B.V. shall under no circumstances accept any operator to make use of its platform services unless it is duly licensed by the Curacao Gaming Control Board.

The company reserves the right to conduct Enhanced Due Diligence (EDD) for which additional documentation may be requested to satisfy end concerns and mitigate the risk accordingly.

Furthermore, Meta Tech Innovations B.V. shall also ascertain that all operators providing remote gaming services through its platform have in place a solid framework of fraud and

Anti-Money Laundering and Counter Funding of Terrorism management procedures. These procedures should be of such a nature to adequately protect the operator from being used as a tool to conduct illicit activity.

(b) Anti-Money Laundering and Counter Funding of Terrorism

The Company shall appoint a Money Laundering Reporting Officer (hereinafter referred to as “MLRO” and shall allow him access to all the information which may be of assistance to him in considering any internal report made to him in relation to the knowledge, suspicion or reason to believe that a person is or may be involved in money laundering or the funding of terrorism or any crime which is deemed to be detrimental to the good standing of the Company.

The MLRO shall consider such report in the light of all relevant information to determine whether or not that information does indeed give rise to a knowledge or suspicion that a person may have been or is engaged in the said activity. Meta Tech Innovations B.V. shall then report any suspicion/knowledge to the Curacao Gaming Control Board, and if necessary to the Financial Intelligence Unit Curacao (hereinafter referred to as “FIU”) and shall also submit any relevant identification or documentation not later than five (5) working days from the day the suspicion first arose.

Any transaction that has raised suspicion shall not be carried out until the necessary report is made to the FIU, unless delay would cause prejudice to the investigation or it is otherwise impossible, and in any such case the FIU is to be informed immediately on the effecting of the transaction. If the MLRO does not report the suspicion to the FIU, the said authorities shall be duly informed of the reasons if they are so requested.

The MLRO also shall make every effort to protect the identity of a person who in good faith reported the suspected fraud. However, disciplinary action may be taken as provided by this policy if a report is made in bad faith.

To avoid Anti-Money Laundering the Company will provide initial and on-going training to all relevant staff so that they are aware of their personal responsibilities and the procedures in respect of identifying operators and service providers, record-keeping and reporting any unusual/suspicious transactions.