



Anti-Money Laundering & Prevention of Crime Policies & Procedures

APPROVALS

All approvals are maintained and controlled in the [Document Control System]

Please refer to the [Document Control System] for the current controlled revision and approval records.

Draft and Archived/Obsolete revisions are not to be used.

Access [Document Control System] system to verify revision.

Version Control				
Version	Date	Security Class	Responsible Person	Purpose
1	27/10/2020	Confidential	Sarah Grech	Creation of Document
1.1	07/12/2022	Confidential	Augusto Quintano	Revision of Document

Contents

1. Objectives	3
2. The Meaning of Money Laundering.....	3
3. Responsibilities.....	3
4. Customer Due Diligence	5
5. Risk Assessment	5
6. Regulatory Impact Assessment.....	6
7. Ongoing Monitoring	7
8. Training	7
9. Record Keeping.....	7
10. Reporting	8
11. Protection of Equipment.....	8
12. Responsible Gaming.....	8
12.1 Introduction.....	8
12.2 Player Protection Directive	9
13. Update of Procedure	10

1. Objectives

The main scope of this document (these “**Policies & Procedures**”) is to establish the essential standards designed to prevent Oracle Gaming Shops Ltd. (the “**Company**”) from being used for money laundering and terrorism financing and the risks faced by the Company in this regard. These Policies & Procedures apply to the Company and all of its staff who provide services which might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.

The engagement of business-to-business gaming operators (“**Operator/s**”) involves the entering into of agreements with such Operators in order to ensure, on a continuing basis, the availability of games provided by the Company to the Operators’ sub-licensees and/or players from various jurisdictions. Such business activity can be defined as one with the potential, if disrupted, to cause harm to the Company’s reputation and profitability.

2. The Meaning of Money Laundering

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. There are three (3) stages in the process:

- i. Placement: cash first enters the financial system at the “placement” stage where the cash generated from criminal activities is converted into monetary instruments.
- ii. Layering: this is how the link between the funds and the criminal is concealed.
- iii. Integration: investing and/or recovering the funds in a way that looks legitimate.

As it is strictly Company policy **not** to accept cash as means of payment, the Company’s Policies & Procedures are focused on preventing the use of the Company’s activities and resources in the 2nd and 3rd stages.

3. Responsibilities

The Finance Department is responsible for monitoring all transactions to and from the Company. The Company’s senior management, as well as all employees, are fully committed to adopting a risk-based approach to anti-money laundering (“**AML**”) and countering terrorist financing (“**CTF**”) with effort focused where it is most needed to be able to process payment transactions in a way free from money laundering issues.

The developed internal systems and procedures applied by the Company are appropriate for remote gaming businesses. The Company appreciates that its money laundering and terrorist financing risk assessment is not a one-off exercise, and these are assessed regularly so that the adopted approach is effective at any time.

3.1. Senior Management Responsibility

Senior management is fully engaged in the processes of the Company's assessment of risks for money laundering and terrorist financing and are involved at every level of the decision making to develop the appropriate policies and processes to comply with relevant legislation including the Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta, the Prevention of Money Laundering and Funding of Terrorism Regulations (S.L. 373.01), the 3rd EU Money Laundering Directive, the 4th EU Money Laundering Directive and the 5th EU Money Laundering Directive (the "**Regulations**") and all required due diligence checks.

3.2. Money Laundering Reporting Officer

The Money Laundering Reporting Officer ("**MLRO**") is responsible for the oversight of all aspects relating to AML and CTF within the Company, has the authority to act independently in carrying out his/her responsibilities and has access to sufficient resources to carry out his/her duties.

The MLRO's duties and responsibilities include:

- identifying money laundering and terrorist financing risks relevant to the Company;
- designing and implementing policies and procedures relating to AML and CTF, monitoring the effectiveness of these policies and procedures and reviewing and updating these policies and procedures;
- reporting to Senior Management on AML and CTF activity and the effectiveness of the Company's controls;
- keeping AML/CTF records;
- training employees to ensure that they are aware of these Policies & Procedures and how to report suspicious transactions;
- being the internal point of contact for the suspicious transaction reports ("**STRs**");
- reviewing and investigating STRs and considering whether a suspicious activity report ("**SAR**") should be submitted to Financial Intelligence Analysis Unit ("**FIAU**") and, where appropriate, making SARs to the FIAU and requesting the necessary consent to proceed with transactions.

Any internal report should be considered by the nominated officer, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing.

Where any AML and/or CTF tasks are delegated within the business, the MLRO will remain responsible for all AML and CTF issues. Any delegated tasks will be recorded and will be counter-signed by the delegate to confirm acceptance of responsibility. Employees who need to be aware of the delegation will be notified immediately.

If the MLRO is temporary unavailable (for example, if on vacation leave, long-term sick leave) the Compliance Manager takes over his duties and responsibilities. Employees then report to their nominated officer when they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist activity. The MLRO or nominated officer must consider each report made to determine whether it gives rise to grounds for knowledge or suspicion.

3.3. Employees' Responsibilities

Employees are trained to follow the Company's policies and procedures for customer due diligence ("CDD"), including enhanced requirements for high-risk customers (enhanced due diligence, or "EDD"), which includes politically exposed persons ("PEPs").

Employees must report to the MLRO any knowledge or suspicion of money laundering whether by Operators, guests or other employees by drafting an internal STR.

4. Customer Due Diligence

Appropriate due diligence must be carried out on Operators before the formation of any contractual relationship with such Operators to ensure suitability, the upholding of industry standards in its selection process, to safeguard consumer protection, to prevent its business from being used for money laundering and terrorist financing as well as to protect its own interests and remain compliant with all applicable laws and regulations.

Identifying an Operator means obtaining information about the Operator's name, company registration number, date & country of incorporation and registered address, amongst other information, and cross checking such information using an electronic verification third party provider. *Verifying* identity means obtaining evidence that supports this information.

To fulfil the necessary CDD process, the Company requires Operators to complete the Due Diligence Form as found under Annex I and provide all the required due diligence documentation as requested therein including, any additional information and/or documentation which the Company may require following review of the completed Due Diligence Form and documentation.

The Company will require Operators to provide the following documentation:

- organizational chart and shareholding structure;
- certificate of good standing;
- certificate of incorporation;
- memorandum and articles of association;
- a copy of a valid license in accordance with section 6;
- documentation pertaining to directors, senior personnel, shareholders and UBOs which will assist the Company to verify the information provided on such individuals in the Due Diligence Form.

If documents are in a foreign language, the Company shall request the Operator to provide it with certified true translations of the same.

5. Risk Assessment

The Company adopts a risk-based approach and thus, Operators which fall to be categorised as low, medium or high risk shall be subjected to different due diligence requirements and checks commensurate to their risk score.

The Company is aware that CDD is ongoing and may need updating where there are changes in an Operator's circumstances and details.

The assessment of risk carried out by the Company is based on a number of factors and questions including:

- what risk is posed by the Operator?
- is the Operator located in a high-risk jurisdiction?
- what is the Operator's length and depth of experience in remote gaming services?
- does the Operator uphold a good reputation?
- is the Operator requesting that the Company's services are to be paid from several bank accounts or a bank account in the name of another entity?
- is the Operator requesting that funds are sent to several bank accounts or a bank account in the name of another entity?
- are any of the personnel involved in the management and financing of the Operator classified as PEPs?

Employees remain vigilant and use their experience and common sense in applying the Company's risk-based criteria and rules, using guidance from the MLRO or nominated officer as appropriate.

6. Regulatory Impact Assessment

The Company is committed to ensuring that contractual arrangements with any Operators do not diminish the Company's ability to fulfil its obligations to other clients and customers or to the Malta Gaming Authority (the "**MGA**") under the Gaming Act, Chapter 583 of the Laws of Malta and all regulations and directives enacted thereunder.

The Company is also committed to ensuring that Operators of the highest standard are chosen. In doing so it does not stop at due diligence documentation but also makes sure that the Operator is in possession of the relevant and required licences and that such licences are still valid and whether it is in possession of any other certification.

The first step in this regard, is to check that potential Operators are in possession of a valid licence issued by:

- i. the MGA;
- ii. the competent regulator in another jurisdiction within the EU/EEA;
- iii. the competent regulator in another reputable jurisdiction with which the MGA has an agreement;
- iv. the competent regulator in another reputable jurisdiction (not being within the EU/EEA) where the Company has justifiable reasons to be satisfied that the Operator is subject to regulatory safeguards and supervision which are comparable to those of the MGA.

The Company shall request the Operator to provide it with a certified true copy of said licence.

7. Ongoing Monitoring

Operators shall be constantly monitored and reviewed as part of the Company's ongoing operations. The monitoring of higher risk Operators is likely to be more frequent and involve greater scrutiny than is appropriate for lower risk Operators. Monitoring of Operators is done by the MLRO.

Such monitoring and review shall involve an assessment of the performance of the Operator and shall take into consideration a number of factors such as:

- the existence of any adverse media involving the Operator;
- the continued validity of a licence;
- any warnings, penalties and/or fines issued against the Operator by any regulator;
- responsiveness and understanding of trends and industry developments;
- communications standards including ability to advise in relation to any issues;
- demonstrated level of expertise;
- pricing and market competitiveness;
- potential conflicts of interest;
- dispute resolution performance;
- disaster recovery performance;
- changes in the business focus; and
- possible impact on regulators assessment of control and risk factors.

8. Training

All relevant employees of the Company are given training on AML and CTF, both at induction and by way of refresher training on an annual basis. The Company ensures that employees understand the Regulations and apply the Company's policies and procedures, including the requirements for CDD, record keeping and STRs/SARs.

The Monitoring & Fraud department consists of employees who are alert to the risks of money laundering and terrorist financing and who are well trained in the identification of unusual activities or transactions that appear to be suspicious.

The MLRO, nominated officers and employees responsible for completing CDD checks are regularly given training in how to recognise and deal with transactions and other activities that may be related to money laundering or terrorist financing.

9. Record Keeping

It is the Company's policy to maintain the following records:

- all communications with Operators including details thereof, via any platform, including which employee/s dealt with the interaction, what was discussed, why an interaction was made and the outcome thereof;
- Due Diligence Form and due diligence documentation;

- risk assessment undertaken for all Operators;
- details of any AML and/or CTF tasks assigned to employees;
- internal reports of the MLRO and its decision when receiving an STR;
- external reports made to the FIAU including decisions made by the FIAU on SARs and the action taken or to be taken by the Company after the FIAU has made their decision;
- details of steps taken to manage and mitigate risks of money laundering and terrorist financing and of crime in general;
- records of training received from external organisations and given to employees.

These records will be kept for a period of at least five (5) years, beginning from the date on which the business relationship ends.

10. Reporting

Where an employee of the Company has received information, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, that employee must make an internal report, an STR, to the MLRO.

Any STRs are considered by the MLRO, in the light of all other relevant information, to determine whether or not the information contained in the report leads them to form knowledge or suspicion, or reasonable grounds for knowledge or suspicion, of money laundering or terrorist financing. Where appropriate, the MLRO will make an SAR to the FIAU and will apply for the appropriate consent required.

11. Protection of Equipment

The Company ensures that its equipment and business is protected from crime and criminal misuses by:

- keeping its premises fully locked when no member of staff is present;
- members of staff accessing the office by using an electronic punch clock. This will allow tracking of staff members in case of illegal activity;
- computer equipment being protected by user-log out and password protected screensavers whenever they are left unattended, or outside office hours;
- CCTV installed throughout the building, keeping the premises secure.

12. Responsible Gaming

12.1 Introduction

Gambling is a form of entertainment and should never be perceived as a means of generating income. Whilst most individuals treat gambling as a recreational activity and spend only what they can afford

to lose, others are unable to do so. It is therefore of the utmost importance that responsible gambling and player protection is high on the agenda of gaming operators.

12.2 Player Protection Directive

The Player Protection Directive (Directive 2 of 2018) sets out various obligations which must be rigorously adhered to. As part of the Directive, operators (B2C), must prominently display on all websites licensed by the Authority:

- The licensee details.
- A sign which indicates that underage gaming is not permissible.
- A 'responsible gaming' message, explaining that gaming can be harmful if it is not controlled, and information about the player support measures on the website.
- Dynamic seal or kite mark.
- A link leading to a webpage or application which includes all relevant responsible gaming information required by the Directive. This information must be clear and intelligible, and within one click from anywhere on the website.
- A link which enables players to refer to one or more gambling help organisations.
- A message before first deposit, providing information and access to available responsible gaming tools and limits.

The responsibilities of a **B2B Licensed entity** are the following:

B2B licensees shall:

(a) display in a readily visible manner a statement that they are licensed by the Authority, together with the licence number and the activities for which they are licensed:

(i) on their website; and

(ii) in premises accessible to the public which are used to showcase to clients or potential clients the products or services which they supply in virtue of the licence issued by the Authority, as may be applicable in each case. Provided that, for the avoidance of doubt, this article is also applicable to licensees that are in possession of a recognition notice issued in terms of regulation 22 of the Gaming Authorisations Regulations and which have their premises located in Malta.

(b) clearly distinguish between the products and, or services:

(i) which are licensed by the Authority;

(ii) which are in possession of a material supply certificate issued by the Authority; and

(iii) which are neither licensed nor in possession of a material supply certificate issued by the Authority.

13. Update of Procedure

The Company's policies and procedures are updated on a regular basis. Any material changes to this document will be advised by senior management either via electronic mail or at our regular staff meetings.

These Policies & Procedures are securely stored on the Company's shared drive (network) which is accessible by all staff. All information can be immediately accessed on the computer network and will be guaranteed to be up to date at all times.