ANTI-MONEY LAUNDERING POLICY

INTRODUCTION

1. It is our policy to carry on business in accordance with the highest ethical standards. This includes complying with all applicable laws and regulations aimed at combating money laundering. This Policy explains our individual responsibility in complying with anti-money laundering ("**AML Laws**") around the world and ensuring that any third parties that we engage to act on our behalf, do the same.

2. The management of ATOG is committed to complying with all laws. Any employee who violates the rules in this Policy or who permits anyone to violate those rules may be subject to appropriate disciplinary action, up to and including dismissal, and may be subject to personal civil or criminal fines.

3. If you have any questions about this Policy you should contact the Compliance Manager.

WHO IS SUBJECT TO THIS POLICY?

4. This policy applies to all individuals working for the company or any Group Company on its behalf in any capacity, including employees at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located (collectively referred to as workers in this policy).

WHAT'S THE RISK?

5. Violations of AML Laws may lead to severe civil and/or criminal penalties against companies and individuals, including significant monetary fines, imprisonment, extradition, blacklisting, revocation of licences, and disqualification of directors.

6. In addition, violations of AML Laws can lead to damaging practical consequences, including harm to reputation and commercial relationships, restrictions in the way we can do business, and extensive time and cost in conducting internal investigations and/or defending against government investigations and enforcement actions.

WHAT IS MONEY LAUNDERING?

7. Money laundering means exchanging money or assets that were obtained criminally for money or other assets that are 'clean'. The clean money or assets don't have an obvious link with any criminal activity.

8. The following types of activities are considered to be "money laundering" and are prohibited under this Policy:

   a) the conversion or transfer of property (including money), knowing or suspecting that such property is derived from criminal or certain specified unlawful activity ("**criminal property**"), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;

   b) conducting a financial transaction which involves criminal property;

   c) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, ownership or control of criminal property;

d) the acquisition, possession or use of criminal property;

e) promoting the carrying on of unlawful activity; and

f) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

9. The broad definition of money laundering means that anybody (including any ATOG employee) could be in violation of the law if he/she becomes aware of, or suspects, the existence of criminal property within the business and becomes involved in or continues to be involved in a matter which relates to that property being linked to the business without reporting his/her concerns.

10. Property can be criminal property where it derives from any criminal conduct, whether the underlying criminal conduct has taken place in the country where you are situated or overseas.

RED FLAGS

11. Where any suspicions arise that criminal conduct may have taken place involving a customer, colleague or third party, you should consider whether there is a risk that money laundering has occurred or may occur.

12. Some examples of red flags to be reported include:

- A customer provides insufficient, false or suspicious information or is reluctant to provide complete information
- Methods or volumes of payment that are not consistent with the payment policy or that are not customarily used in the course of business, e.g., payments with money orders, traveller's cheques, and/or multiple instruments, and payments from unrelated third parties
- Receipts of multiple negotiable instruments to pay a single invoice
- Requests by a customer or partner to pay in cash
- Early repayments of a loan, especially if payment is from an unrelated third party or involves another unacceptable form of payment
- Orders or purchases that are inconsistent with the customer's trade or business
- Payments to or from third parties that have no apparent or logical connection with the customer or transaction
- Payment to or from countries considered high risk for money laundering or terrorist financing
- Payments to or from countries considered to be tax havens or offshore jurisdictions
- Payments from countries unrelated to the transaction or not logical for the customer
- A customer's business formation documents are from a tax haven, or a country that poses a high risk for money laundering, terrorism or terrorist financing, or a country that is not logical for the customer
- Overpayments followed by directions to refund a payment, especially if requested to send the payment to a third party
- Any customer for whom you cannot determine the true beneficial owner
- Structuring transactions to avoid government reporting or record keeping requirements

- Unusually complex business structures, payment patterns that reflect no real business purpose

- Wire transfer activity that is not consistent with the business activities of the customer, or which originates or terminates with parties unrelated to the transaction

- Unexpected spikes in a customer's activities

The above is not intended to be an exhaustive list. Deviation from customer and accepted business practice should alert you to further investigate the activity in accordance with this Policy.

COMPLIANCE

13. Management is responsible for ensuring that their business has a culture of compliance and effective controls to comply with AML laws and regulations to prevent, detect and respond to money laundering and to communicate the serious consequences of non-compliance to employees.

EMPLOYEE RESPONSIBILITY

14. You have the obligation to read and follow this Policy, to understand and identify any red flags that may arise in their business activities and to escalate potential compliance concerns related to AML to the Compliance Manager without notifying anyone involved in the transaction and should not take any actions prior to receiving advice and/or instructions.

DUE DILIGENCE AND RECORD KEEPING

15. It is our policy to carry out due diligence ("**DD**") at the outset of any business relationship and, if necessary, where any red flags arise subsequently on our suppliers, distributors, counterparties, agents and any person with whom ATOG has an established business relationship that will involve the transfer to or receipt of funds, so we can be satisfied that they are who they say they are and so that we can ensure that there are no legal barriers to working with them before contracts are signed or transactions occur. Various factors will determine the appropriate forms and levels of screening.

16. You should escalate any instances where you have cause for suspicion as a result of carrying out DD and ongoing monitoring to the Compliance Manager, who will advise them regarding which tools and processes should be used to facilitate appropriate screening.

17. You must, in consultation with the Compliance Manager, carefully consider screening outcomes before deciding whether to do business with the third party.

18. Record-keeping is an essential component of the audit trail required to assist in any investigation. You must maintain records as evidence of the DD and ongoing monitoring undertaken.

NON-COMPLIANCE

19. Any employee who breaches this policy will face disciplinary action, which could result in dismissal. We reserve our right to terminate our contractual relationship with other workers if they breach this policy.

UPDATES, REVIEW AND OWNERSHIP

20. The Compliance Manager will monitor the effectiveness and review the implementation of this policy on an annual basis, considering its suitability, adequacy and effectiveness. The policy will be re-circulated to all workers who will be required to re-certify their compliance. Any improvements identified will be made as soon as possible. Internal control systems and

procedures will be subject to regular audits to provide assurance that they are effective in countering money laundering.

21. All workers are responsible for the success of this policy and should ensure they use it to disclose any suspected danger or wrongdoing.

22. Workers are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Compliance Manager.

23. This policy does not form part of any employee's contract of employment and it may be amended at any time.