Disclaimer

The material and information contained within this document is for general information and guidance purposes only. Security in Complex Environments Group (SCEG) and ADS Group do not accept any liability or responsibility for any situation arising out of the content contained hereof. Any reliance you place on such material is therefore strictly at your own risk.

GOVERNANCE POLICY

Table of Contents

1. ABOUT THIS POLICY

1.1 This policy is intended to outline the practices and processes by which [COMPANY NAME] is directed and controlled. The owners of [COMPANY NAME] (the "Company") assign to the Board of Directors, ("the Board") the oversight, effective and efficient running of the Company, through compliance with these corporate good practices.

1.2 This policy is written with the intention of sustainable and positive growth.

2. ROLE OF THE BOARD

2.1 The role of the Board of Directors of the Company is the protection and development of long-term shareholder value.

2.2 The Board is responsible for representing the shareholders for overall corporate governance practices of the Company and in the future its subsidiaries. This responsibility includes the overall management of the company including the strategic direction, management goals and performance. The Board acts on authority under the Company's Articles of Association.

2.3 Occupational health and safety standards and management systems are monitored and reviewed by the Board to achieve high standards of performance and compliance with regulations; and business transactions are properly authorised and executed.

2.4 The performance of all directors is to be reviewed by the Board each year.

3. COMPOSITION OF THE BOARD

3.1 The Board currently comprises [NUMBER] directors. In the future the number of directors may increase and should comprise a mix of experience, qualification and gender diversity to enhance future growth and shareholder value.

3.2 When appointing new members to the Board, consideration must be given to seek qualities that enhance the effectiveness of the Board and must:

3.2.1 Be honest, fair and conduct themselves ethically.

3.2.2 Ensure the Company's policies and procedures

3.2.3 Ensure a respectful working environment free from discrimination or harassment of sort.

3.2.4 Ensure the Company avoid actual or apparent conflict of interest

3.2.5 Protect Company assets including its information

3.2.6 Promptly report and resolve any violation of this Policy

3.3 It is the policy of the Company, that when considering the appointment of new directors, the Company should:

3.3.1 Undertake appropriate checks before appointing a person putting forward to security holders a candidate for election.

3.3.2 Provide security holders with all material information in its possession relevant to the decision on whether or not to elect or re-elect a director.

4. DIRECTOR RESPONSIBILITIES

4.1 It is a director's responsibility to:

4.1.1 Manage the Company on a day to day basis

4.1.2 Act only in accordance with the company's constitution and only exercise powers for the purposes for which they are conferred

4.1.3 To act in a way they consider, in good faith, would be most likely to promote the success of a company for the benefit of its members as a whole.

4.1.4 Exercise independent judgement in that they must not fetter their own discretion.

4.1.5 Exercise reasonable care, skill and diligence.

4.1.6 Ensure that full accounts are produced for each financial year.

4.1.7 Not to approve the accounts unless they are satisfied that they give a true and fair view of the assets, liabilities, financial position, and profit and loss of the company.

4.1.8 File the accounts and directors report that each financial year at Companies House.

4.1.9 Make a recommendation for the payment of a dividend to the company shareholders if there are sufficient distributable profits available.

4.1.10 Compare annually Company's corporate governance practices against those recommended or required by any applicable regulator. The Directors must ensure the Company meets all requirements, and where the Company's practices differ from recommended practices, recommend to the Board whether this situation continues to be in the best interests of the Company.

4.1.11 Develop for Board approval any annual and/or interim reports of the Company's governance practices. This report shall include adequate detail to meet or exceed any regulatory or legal governance disclosure requirements, in addition to any additional disclosure the Board deems important.

4.1.12 Consider the Board's short-term needs and longer-term succession plans.

4.1.13 Recommend any reports on corporate governance that may be required or considered advisable.

4.1.14 Undertake such other corporate governance initiatives as may be necessary or desirable to contribute to the success of the Company.

5. CONFLICTS OF INTEREST

5.1 Each director has a statutory duty, a fiduciary duty and an implied duty of loyalty to the Company and, in certain circumstances, to its shareholders to avoid actual or potential conflicts of interests, as well as the duty to act in good faith in the performance of his or her duties as an director.

5.2 If an actual or potential conflict of interest develops, whether because of a change in the business operations of the Company or a subsidiary, or in a director's circumstances, or otherwise, the director should report the matter immediately to the Board for evaluation.

5.3 A significant and potentially ongoing conflict must be resolved, or the director should resign

5.4 If a director has a personal or business interest in a proposed transaction, arrangement or other matter before the Board involving the Company, or an existing transaction or arrangement with the Company, the director shall disclose the interest to the Board (to the extent not already disclosed) and excuse himself or herself from participation in the related deliberations and shall abstain from voting on the matter

5.5 On at least an annual basis, each director shall present to the Board a declaration of interests, setting forth such director's business affiliations with third parties. Each declaration of interests shall include, without limitation, any relationship between the directors and any entities (other than the Company) with which any other directors and/or officers are affiliated, as a potential or actual conflict of interest could arise in such situations.

5.6 Each director shall present to the Board an updated declaration of interest promptly after entering into a new affiliation or changing a pre-existing affiliation. The Secretary shall keep a register of the declarations of interests made by the directors, and such register shall be reviewed by the Board from time to time and at least annually for completeness and accuracy.

6. BOARD MEETINGS

6.1 The Board will hold meetings at least annually [OR insert frequency or number] and any additional meetings. The record of each Board meeting shall be approved by the Chair and circulated to Directors within 2 weeks of the meeting. All meeting may be conducted via any virtual means, as may be expedient and agreed by the directors as acceptable. From time to time consultants may be invited as required to Board Meetings however any discussion on management issues or matters of risk and sensitivity will be conducted with only Directors present.

6.2 Directors are expected to devote sufficient time and attention to prepare for, attend and participate in Board meetings and meetings of committees on which they serve, including advance review of pre-meeting agenda materials circulated prior to each meeting.

6.3 Although the Chair of the Board shall establish the agenda of each Board meeting, all

other Board members are encouraged to suggest items for inclusion on the agenda. Each director is free to raise subjects that are not on the meeting agenda

7. ACCESS TO ADVICE

All Directors have unrestricted access to company records and information except where the Board determines that such access would be adverse to the Company's interests. All Directors may consult employees as required to enable them to discharge their duties as Directors. The Board, or individual Directors may seek independent external professional advice as considered necessary at the expense of the Company, subject to prior consultation with the Chair. A copy of any such advice received is made available to all members of the Board.

8. CODE OF CONDUCT

8.1 The purpose of this code is to prevent behaviour that could harm the company's reputation and standing and seeks to promote:

8.2 Adherence with the objectives set out in the code and all of the company's set policies.

8.3 Ethical conduct including any outside interests that could conflict with, have the potential to conflict, or could be perceived to conflict with the interests of the Company.

8.4 Compliance with all regulatory reporting, respecting the law, honouring the company's internal policies, maintain transparency and ensure all filings are made and disclosed accurately and timely and in accordance with listed exchange, governmental laws and regulations.

8.5 Promoting a self and safe workplace and efforts to contribute to sustainable development with the highest standards or ethics and professionalism.

8.6 Encouragement of disclosure of any violations of the code with clear guidelines and assurance of an open-door policy.

8.7 Applicability. The code applies to all staff, directors and contractors or consultants. Newly hired employees and newly elected directors must sign an acknowledgement that they have understood and read the policy. From time to time there may also be a requirement to re-certify compliance with this policy.

9. CORPORATE SOCIAL RESPONSIBILITY

9.1 The Company Corporate Social Responsibility (CSR) policy outlines the Companies efforts to contribute to legal and sustainable development. It may also refer to suppliers and partners. We want to be a responsible business that meets the highest standards of ethics and professionalism. Our company's social responsibility falls under two categories; compliance to our company's commitment to legality and to observe business social values

and proactivity to promote human rights.

9.2 Compliance. The Company will:

9.2.1 Respect the law.

9.2.2 Honour its internal policies.

9.2.3 Ensure that all its business operations are legitimate.

9.2.4 Keep every partnership and collaboration open and transparent.

9.3 Business and Social Values. The Company will always conduct business with integrity and respect to human rights. We will promote:

9.3.1 Safety and fair dealing.

9.3.2 Respect for the client.

9.3.3 Anti-bribery and anti-corruption practices.

9.3.4 The safety of our employees, our client and their community.

9.3.5 The support of diversity and inclusion.

9.4 The Company is dedicated to protecting human rights. We are a committed equal opportunity employer and will abide by all fair employment practices. We will ensure that our activities do not directly or indirectly violate human rights in any country (e.g. modern slavery).

9.5 Reporting breaches of the CSR. It is essential to ensure that all individuals with concerns feel they are able to freely come forward and that the Company will act in accordance with its policy offering anonymous reporting and non-retaliation for reporting. Employees do not have to reveal their identity in order to make a report. If they do reveal their identity, it will not be disclosed unless disclosure is unavoidable during an investigation.

9.6 In order to ensure a safe and fair working environment is maintained for individuals the company will not take or threaten any action against an employee as a reprisal or retaliation for making a complaint or disclosing or reporting information in good faith. However, if a reporting individual was involved in improper activity the individual may be appropriately disciplined even if they were the one who disclosed the matter to the Company. In these circumstances, the Company may consider the conduct of the reporting individual in reporting the information as a mitigating factor in any disciplinary decision.

10. PERSONAL BEHAVIOUR

10.1 Directors must carry out their duties honestly and responsibly and may not take for themselves personally any opportunities arising from use of the Company's property or information. They may not use company property for personal gain, or profit from an opportunity that may otherwise be available to the company. A duty of care is owed to the Company and its shareholders to advance the company's legitimate interests and to not make personal gain and profit as a result of their employment.

10.2 Directors must refrain from any misconduct relating to alcohol, illegal drugs or other prohibited substances, including legal drugs which may impact the ability to perform duties whilst on Company premises or representing the company, which could affect personal work performance or safety and well-being of themselves or others.

10.3 Directors are responsible for maintaining adequate security over the company's assets, property, resources and information, including being responsible for the proper management of expenditure of the Company's funds. The Company's assets must only be used for appropriate business purposes and must not be sold, misused or transferred without correct authorization.

10.4 Directors and employees should represent the Company fairly and with integrity and should not abuse their position to take unfair advantage of anyone by way of manipulation, concealment or misrepresentation or any other unfair dealing practice.

10.5 Directors and employees should carry out their duties in a transparent manner in good faith and in compliance with the Company's policies and procedures maintaining confidentiality of personal and official information.

11. STATUS OF STAFF

11.1 The Company will or will not issue employment contracts based on the premise of one of two categories:

11.2.1 If the individual is deemed to be an employee.

11.2.2 If the individual is deemed to be self-employed (an independent contractor) and therefore a consultant.

11.2 The contracts should, at the beginning, clearly state which of the two categories above the contract is issued under, in order to establish the relationship between the Company and the individual. In respect of 11.2.1, the following should always be covered/considered:

11.2.1 If the contract worker is an employee, the contract should outline the following:

11.2.2 The job title and basic job requirements the individual is being hired to carry out.

11.2.3 The beginning and end date of employment.

11.2.4 The hours and location of work.

11.2.5 The rate of pay and pay periods.

11.2.6 Deductions that will apply such as any applicable tax.

11.2.7 Benefits that will be provided.

11.3.8 Confidentiality obligations.

11.3.9 Requirement to abide by all company policies.

11.3 If the individual is self-employed (consultant) the contract should, in respect of 11.2.2 outline the following:

11.3.1 The nature of the work to be completed (avoiding any implication of control over how the work will be accomplished or the hours and location of work).

11.3.2 That the relationship is not employer-employee.

11.3.3 That the contractor is responsible for all source deductions such as any applicable tax.

11.3.4 The fees and payment schedule.

11.3.5 The terms for terminating the contract (notice period for termination before completion of the contract, reasons required/not required for terminating the contract prior to completion; payment obligations when terminating before completion of the contract).

11.3.6 Confidentiality obligations.

11.3.7 Requirement to abide by all company policies.

12. IT SECURITY AND PROTECTION

12.1 Monitoring Electronic Communications. The Company will monitor the use of phone, Internet, fax or emails in the workplace. This includes the use of email addresses and phones and other IT equipment such as laptops supplied by us. We will only do this for the following reasons:

12.2 To establish facts which are relevant to the business, to check that procedures are being followed, or to check standards, for example, listening into phone calls to assess quality of work.

12.2.1 To prevent or detect crime.

12.2.3 To check for unauthorised use of telecommunications systems, such as use of the internet or email for personal use.

12.2.4 To make sure electronic systems are operating effectively, for example to prevent computer viruses entering the system.

12.2.5 To check whether a communication received, such as an email or phone call is relevant to the business. In this event we may open emails or listen to voicemails, but we will not record them.

12.2.6 In the interests of client security.

12.3 Electronic Storage. All files, documents or any electronic information relating to a client matter will be stored on a secure storage server at locations known to the Directors. It is not permitted to store such electronic material on a computer desktop or hard drive other than for a short period of time that in any event should not go beyond a working day in length. [This file storage system will be accessed through an external VPN and access to it placed onto the Company supplied laptops or Consultants laptops. Access

through this external VPN, will be controlled via password and authentication software and through an SSL. The files system will be a basic system of folders for each client. Where possible all documents will be generated electronically.] Control will rest with [insert here, name or position] from the [the Company's registered address or [address]]. All such communication will then be copied over to client files, which will be on the same server.

12.4 Logging in to the Company's server will be by using a username, password and authenticator app. Login's will be recorded as will movement of clients' data within the Server. Staff will only be granted access to files they are required to use for their own work. This system of control will be carried out by [name or position].

12.5 Encrypted backups are automatically performed daily and externally in order to avoid redundancy and protect client data and all the Company's files and data. [Name or position] controls this process.

12.6 Where a Consultant utilises their own laptop for processing of work on behalf of the Company, the Consultant will be required to demonstrate the laptop is their own and in singular and complete control of the laptop or other computer type device.

12.7 Directors, consultants and staff will be expected to maintain the highest possible levels of IT and data security. Separate guidance is provided to all staff and consultants at schedules 25 to 27 of the Staff Handbook. There is also a social media policy at Schedule 28 although it does not full cover personal security online. We advise all staff to be aware of their digital footprint and recommend that it is minimised.

12.8 Anti- Malware/ Virus Software. The Company utilises an anti-malware and virus software [called _____ , go to____WEBSITE____]to find out more about it. The Company will provide the licence to staff or consultants accessing the Company Storage system on a daily basis. Once the licence is provided, staff and consultants will be required to install [_____]on all their devices (laptops, computers, tablets, mobile phones etc) used to access their emails and sensitive information. The [_____] should be set to update and automatically scan files upon access. In addition, you should perform a scan of files daily to ensure that you comply with the Company's cyber protection.

13. PASSWORDS

Any staff accessing the Company data storage system, email systems or any other electronic system that belongs to the Company is required to have a minimum password complexity of 8-10 characters using upper and lower-case letters, numbers and symbols. Under no circumstances should passwords be disclosed to any other person or shared by any means whatsoever (except when being initially provided). Once you have been provided with a password or set a password, any reference to it, including the means by which it was passed to you such as email, should be deleted. Passwords must be changed every 60 days.

14. CLIENT DUE DILIGENCE

14.1 Due diligence is required for all new clients before establishing a business relationship or carrying out a transaction. This is appropriate where there is opportunity or risk of our services or the client becoming involved in money laundering or terrorist financing. Under Article 11 of Money Laundering Directive 4, the Company must apply Customer Due Diligence measures when:

a) Establishing a business relationship (Article 3(13) of MLD4)

b) Carrying out an occasional transaction that either:

i) amounts to EUR15,000 or more, whether the transaction is carried out in a single operation or in several operations that appear to be linked; or

ii)constitutes a transfer of funds exceeding EUR1,000

c) There is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold.

d) There are doubts about the veracity or adequacy of previously obtained customer identification data.

14.2 The exceptions to this, unless there has been a significant change in any factor of the business and/or programme, are when:

14.2.2 The proposed opportunity is a continuation of funding or development of an existing project;

14.2.3 A recent due diligence assessment, within the last [one year], has been carried out on the proposed partner/project and where this assessment relates to activities in a similar or related sphere of activity.

14.3 There are three levels of customer due diligence: standard, simplified and enhanced.

14.4 Standard customer due diligence. This involves identifying the customer, and ensuring it is based on a reliable independent source. The purpose and intended nature of the business relationship or transaction must be assessed and further information obtained where appropriate.

14.5 Simplified customer due diligence. This can be applied when a risk assessment has shown a negligible or low risk of money laundering. The only requirement is to identify the customer and there is no need to verify the customer's identity.

14.6 Enhanced customer due diligence. Enhanced CDD must be applied when the risk of money laundering is high, such as if the person in question is a politically exposed person. Enhanced due diligence measures can include:

14.6.1 Additional identification information from the customer
Information on the source of funds or source of wealth

14.6.2 The intended nature of the business relationship

14.6.3 The purpose of the transaction

14.6.4 Subjecting the customer to additional ongoing monitoring procedures

14.7 Due Diligence requires that the following is obtained:

14.7.1 Identify and verify the client's identification
14.7.2 If there is a beneficial owner (those controlling more than 25% of a business) who is not the client, take measures to verify who the beneficial owner is
14.7.3 Obtain Information on the purposes and intended nature of the business relationship.

14.8 Enhanced due diligence. All clients who fall under the following categories must be subjected to enhanced due diligence:

14.8.1 the client is not dealt with face to face;
14.8.2 the client is a politically exposed person (PEP), this applicable to domestic or foreign PEP and also apply to family members and persons known to be close associates of PEPs;
14.8.3 the client is an entity or/and a natural person from high-risk third countries nominated by the Commission in delegated acts
14.8.4 there is any other situation which can present a higher risk of money laundering or terrorist financing;
14.8.5 where there is general suspicion of the client activities or conduct;
14.8.6 the business relationship is conducted in unusual circumstances;
14.8.7 legal persons or arrangements that are personal asset-holding vehicles;
14.8.8 companies that have nominee shareholders or shares in bearer form;
14.8.9 businesses that are cash-intensive;
14.8.10 the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

14.9 All product, service, transaction or delivery channel risk factors who fall under the following categories must be subjected to enhanced due diligence:

14.9.1 private banking;
14.9.2 products or transactions that might favour anonymity;
14.9.3 non-face-to-face business relationships or transactions, without certain
14.9.4 safeguards, such as electronic signatures;
14.9.5 payment received from unknown or unassociated third parties;
14.9.6 new products and new business practices, including new delivery
14.9.7 mechanisms, and the use of new or developing technologies for both new and pre-existing products.

14.10 All clients who fall under the geographical risk-factors below must be subjected to enhanced due diligence:

14.10.1 countries identified by credible sources, such as mutual evaluations detailed assessment reports or published follow-up reports, as not having effective AML or CTF systems;
14.10.2 countries identified by credible sources as having significant levels or corruption or other criminal activity;
14.10.3 countries subject to sanctions, embargos or similar measures issued by, for example, the EU or the United Nations;

14.10.4 countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

14.11 These are non-exhaustive lists of factors and types of evidence of potentially higher-risk situations set out in Annex III to MLD4 (*Article 18(3), MLD4*).

15. THIRD PARTY SUPPLIERS

15.1 There will be no discrimination, directly or indirectly in relation to the groupings listed in this manual below regarding the selection and instruction of any provider of third-party services (supply chain). This paragraph forms the policy in place and available to all staff covering the instruction of any third party precluding any form of discrimination either directly or indirectly on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. Any staff member breaching this policy may be subject to internal disciplinary action if appropriate and the matter may be reported to any relevant professional body.

15.2 Importance will be placed on the need to ensure our supply chain is as free of the risk of fraud, people trafficking (including slavery) along with paying of invoices promptly whilst ensuring integration of our policies in day to day interaction with suppliers.

16. BUSINESS CONTINUITY AND SUCCESSION PLANNING [Insert if required]

17. TRAVEL, SUBSISTENCE AND CLAIMS POLICY [Insert if varied from/not covered in the Staff Handbook]