DATA PROTECTION POLICY

1. INTRODUCTION

This Policy set out the measures which African Marine Solutions Group (Pty) Ltd, a private limited company duly registered under the company laws of South Africa with its registered place of business at 31 Carlisle Street, Paarden Eiland, 7405 (hereafter referred to as the "Company") in its capacity as a Responsible Party must implement regarding the regulation and protection of its stakeholders, employees, contractors, agents and any other individual or legal entity's (hereinafter referred to as "Data Subjects") Personal Information in terms of the Protection of Personal Information Act No 4 of 2013 (hereinafter referred to as "POPIA").

The Policy sets out the Company's measures regarding the collection, processing, transfer and storage of Personal Data. The procedures and principles set out in this Policy must be followed at all times by the Company, its stakeholders, directors, employees, contractors and any other parties working on behalf of the Company.

2. DEFINITIONS

"Consent"	means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
"Company"	means African Marine Solutions Group (Pty) Ltd.
"Data Subject"	means the person to whom personal information relates to
"De-Identify"	means, in relation to personal information of a data subject, to delete any information that: • identifies the data subject; • can be used or manipulated by a reasonably foreseeable method to identify the data subject; or • can be linked by a reasonably foreseeable method to other information that identifies the data subject; and • "de-identified" has a corresponding meaning.
"Electronic Communication"	means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
"Person"	means a natural or juristic person.
"Personal Information"	means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to: • information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; • information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person; • the biometric information of the person; • the personal opinions, views or preferences of the person; • correspondence sent by the person that is implicitly or explicitly

	of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about the person; and • the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
"POPIA"	means the Protection of Personal Information Act, No 4 of 2013.
"Processing"	means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; • dissemination by means of transmission, distribution or making available in any other form; or • merging, linking, as well as restriction, degradation, erasure or destruction of information.
"Record"	means any recorded information: regardless of form or medium, including any of the following: • writing on any material; • information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; • label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; • book, map, plan, graph or drawing; • photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; • in the possession or under the control of the responsible party; • whether or not it was created by the responsible party; and • regardless of when it came into existence.
"Re-Identify"	means, in relation to personal information of a data subject, to resurrect any information that has been de-identified, that: • identifies the data subject; • can be used or manipulated by a reasonably foreseeable method to identify the data subject; or • can be linked by a reasonably foreseeable method to other information that identifies the data subject; • and "re-identified" has a corresponding meaning.
"Responsible Party"	means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
"Special Personal Information"	means personal information relating to: • the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of the data subject; or • the criminal behaviour of a data subject to the extent that such information relates the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. SCOPE

3.1 The Company collects and uses Personal Information of stakeholders, employees, contractors, agents and any other individual or legal entity with whom it works in order to operate and to carry out its business effectively. The Company regards the lawful and appropriate processing of all Personal Information as important. The Company therefore fully endorses and adheres to the principles of POPIA.

3.2 All executives and managers are responsible for ensuring that all employees, agents, contractors or

other party acting on behalf of the Company, comply with this Policy and where necessary, implement such practices, processes, controls and training in order to comply with such compliance.

4. DATA RETENTION AND RESTRICTION

4.1 The Company shall collect Personal Information for a specific and explicitly defined and lawful purpose related to its functions or activities and it shall inform the Data Subject thereof.

4.2 The Company shall not retain any Personal Information for any longer than it is necessary in light of the purposes for which it was originally collected, held, stored or subsequently processed. This may include if retention is authorised by law, the record is required for lawful purposes related to its functions or activities or it is required by a contract between the parties.

4.3 The Company may retain records of Personal Information for periods in excess of those contemplated in clause 4.2 above if it is for historical, statistical or research purposes provided that the Company has established the necessary and appropriate safeguards against the records being used for other purposes.

4.4 The Company shall destroy or delete a record of Personal Information or De-Identify it as soon as reasonably practicable after the Company is no longer authorised to retain the record in terms of clause 4.2 or 4.3 above. The record shall be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form.

4.5 The Company shall restrict processing of any Personal Information if the accuracy of the Personal Information is contested by the Data Subject, for a period enabling the Company to verify the accuracy of the information. Such Personal Information shall be further restricted if the processing is unlawful and the Data Subject opposes its destruction or deletion and requests that it be restricted.

4.6 The Company shall restrict processing of any Personal Information if the information is no longer required for the purpose it was collected or subsequently processed, but it has to be maintained for purposes of proof.

5. SECURITY MEASURES ON INTEGRITY AND CONFIDENTIALITY OF DATA

The Company must secure the integrity and confidentiality of Personal Information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent the either the loss of, damage to or unauthorised destruction of Personal Information or the unlawful access to or processing of Personal Information.

6. DATA PROTECTION MEASURES

6.1 The Company shall ensure that its employees, agents and contractors or any other party working on its behalf comply with the following when working with Personal Information:

- 6.1.1 all emails containing Personal Information must be encrypted using industry standard methods;
- 6.1.2 all emails containing Personal Information must either be marked "confidential" or contain a disclaimer that the contents of the email are "confidential";
- 6.1.3 Personal Information may be transmitted over secure networks only;
- 6.1.4 all Personal Information which is transferred physically, including that on removable electronic media, shall be transferred in a suitable folder marked "Confidential";
- 6.1.5 where any confidential or Personal Information is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the User must lock the computer and screen before leaving it;
- 6.1.6 where any Personal Information is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies of Personal Information to be discarded, should be shredded, and electronic copies should be deleted securely using standard methods;
- 6.1.7 Personal Information must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;
- 6.1.8 all Personal Information which is stored electronically should be backed up weekly with backups stored onsite and/or offsite. All backups should be encrypted using industry standard methods;
- 6.1.9 all electronic copies of Perosnal Information should be stored securely using passwords and industry standard data encryption; and
- 6.1.10 all passwords used to protect Personal Information should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. Under no circumstances should any passwords be written down or shared between any employees, agents,

contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method as assisted by the IT Department.

7. ORGANISATIONAL MEASURES

7.1 The Company shall ensure that the following measures are taken with respect to the collection, holding and processing of Personal Information:

- 7.1.1 all employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the under this Policy;
- 7.1.2 only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, Personal Information in order to carry out their assigned duties correctly shall have access to Personal Information held by the Company;
- 7.1.3 all employees, agents, contractors, or other parties working on behalf of the Company handling Personal Information will be appropriately trained to do so;
- 7.1.4 all employees, agents, contractors, or other parties working on behalf of the Company handling Personal Information will be appropriately supervised;
- 7.1.5 methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;
- 7.1.6 the performance of those employees, agents, contractors, or other parties working on behalf of the Company handling Personal Information shall be regularly evaluated and reviewed;
- 7.1.7 all employees, agents, contractors, or other parties working on behalf of the Company handling Personal Information will be bound to do so in accordance with this Policy;
- 7.1.8 all agents, contractors, or other parties working on behalf of the Company handling Personal Information must ensure that any and all of their employees who are involved in the processing of Personal Information are held to the same conditions as those relevant employees of the Company arising out of this Policy;
- 7.1.9 where any agent, contractor or other party working on behalf of the Company handling Personal Information fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

8. TRANSFER OF PERSONAL DATA TO A COUNTRY OUTSIDE OF SOUTH AFRICA

8.1 The Company may from time to time transfer ('transfer' includes making available remotely) Personal Information to other countries;

8.2 The transfer of Personal Information to another country shall take place if one or more of the following applies:

- 8.2.1 is to a country that ensures an adequate level of protection for Personal Information;
- 8.2.2 is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; which includes standard data protection clauses;
- 8.2.3 is made with the informed consent of the relevant Data Subjects;
- 8.2.4 is necessary for the performance of a contract between the Data Subject and the Company;
- 8.2.5 is necessary for important public interest reasons;
- 8.2.6 is necessary for the conduct of legal claims; or
- 8.2.7 is necessary to protect the vital interests of the Data Subject or other individuals where the Data Subject is physically or legally unable to give their consent.

9. FOREIGN COUNTRIES NOT SUBJECT TO ANY DATA PROTECTION LAWS AND/OR REGULATIONS

9.1 In the event that the Company transfers Personal Information to a foreign country where there is no EU declaration of adequate safeguards and/or where juristic personal information is processed), it shall ensure that it:

- 9.1.1 carries out due diligence checks of the data protection laws (if any) that are in place in the foreign country that they wish to export the Personal Information to;
- 9.1.2 obtains advice on the laws in that foreign country that permit access to Personal Information by government agencies; and
- 9.1.3 puts in place the appropriate safeguards in comprehensive data-transfer agreements through the use of properly worded Standard Contractual Clauses (that set safeguard standards for the transfer of Personal Information) or binding corporate rules (which would only apply to transfers of Personal Information within a group of companies).

10. DATA BREACH NOTIFICATION

10.1 All Personal Information breaches must be reported immediately to the Company's Information Officer;

10.2 If a breach of Personal Information occurs and that breach is likely to result in a risk to the rights and freedoms of Data Subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Information Officer must ensure that the Company is made aware of the breach and that it is remedied without delay;

10.3 In the event that a breach of Personal Information is likely to result in a high risk (that is, a higher risk than that described under clause 10.2 above, to the rights of the Data Subjects, the Information Officer must ensure that all affected Data Subjects are informed of the breach directly and without undue delay;

10.4 A notification regarding a data breach shall include the following information:

- 10.4.1 the details of the Data Subject which has been affected by the breach;
- 10.4.2 the nature of the Personal Information breached;
- 10.4.3 the likely consequences of the breach;
- 10.4.4 the details of the preventative measures taken to contain the breach and the recovery measures taken, or to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects; and
- 10.4.5 the notification shall be validated by the Information Officer.

11. DIRECT MARKETING

11.1 Direct marketing, including unsolicited direct electronic marketing is prohibited unless the Data Subject has consented to the receipt of this marketing material.

11.2 In order to ensure that direct marketing is sent out in a lawful manner, all Personnel must ensure that:

- 11.2.1 all of the Company's customers, when approached or dealt with for the first time, are given the opportunity in an informal manner to agree or disagree to the receipt of any of the Company's direct marketing material, if applicable;
- 11.2.2 before direct marketing is sent to a non-customer that such person provides his, her, or its consent thereto;
- 11.2.3 when marketing material is sent to Data Subjects, the Company must allow Data Subject the ability to opt out of any further marketing material; and
- 11.2.4 when a Data Subject exercises his, her or its right to object to receiving direct marketing, in the form then this shall be recorded and given effect to and no further direct marketing shall be sent to a Data Subject that has opted out of receiving any direct marketing from the Company.

12. REPORTING BREACHES OF PERSONAL INFORMATION

12.1 In the event of a breach of any Personal Information, the Company has a duty to give notice of such breach to the Information Regulator in the case of a breach in South Africa and to the affected Data Subjects.

12.2 The Company has put in place appropriate procedures to deal with any breaches of Personal Information and will promptly notify the Information Regulator and / or the affected Data Subjects, as the case may be when it is legally required to do so.

12.3 In the event of a breach of Personal Information, the Company has a duty to immediately report through to the Information Officer, any suspected or known Personal Information breach in the form of a report which shall include details in respect of the categories and approximate number of Data Subjects concerned; categories and approximate number of Personal Information records concerned; the likely cause of and the consequences of the breach; details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects; keep such information strictly private and confidential; not to deal with any persons in relation to the Personal Information breach, including any officials to investigators, noting that only the with the approval of the Company's Board has the right to report any Information Officer Personal Information or security breach to the Information Regulator and or the affected Data Subjects, as the case may be.

13. ACCEPTANCE AND BINDING NATURE OF THIS DOCUMENT

13.1 By providing the Company with the Personal Information which it requires from a Data Subject, the Data Subject:

- 13.1.1 acknowledges that he/she understands why his/her Personal Information needs to be processed;

13.1.2 accepts the terms which will apply to such processing, including the terms applicable to the transfer of such Personal Information cross border;

13.1.3 where consent is required for any processing as reflected in this Processing notice, the Data Subject agrees that the Company may process this particular Personal Information.

13.2 Where a Data Subject provides the Company with another individual or legal entity's Personal Information for processing, the Data Subject confirms that that he/she has obtained the required permission from such individual or legal entity to provide the Company with their/its Personal Information for processing.

13.3 The rights and obligations of the parties under this Processing Notice will be binding on, and will be of benefit to, each of the parties' successors in title and / or assigns where applicable.

13.4 Should any of the Personal Information concern or pertain to a legal entity whom the Data Subject represents, the Data Subject confirms that he/she has the necessary authority to act on behalf of such legal entity and that he/she has the right to provide the Personal Information and/ or the required permissions in respect of the processing of that company, organisation or entity's Personal Information.

14. IMPLEMENTATION OF POLICY

This Policy shall be deemed to be effective as of 30 June 2021. No part of this Policy shall have a retroactive effect and will only apply to matter occurring on or after this date.

15. CONTACT

If you have any comments or questions regarding this Website Privacy Policy or on the Company's data handling practices, or wish to contact our Information Officer, please contact her at p.ngcobo@amsol.co.za