PRIVACY POLICY

1. INTRODUCTION

This Policy sets out the measures which African Marine Solutions Group (Pty) Ltd [AMSOL], 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") as a Responsible Party must implement regarding the regulation and protection of Employees' 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 relating to all Data Subjects. The procedure and principles set out in this Policy must be followed at all times by the Company.

2. DEFINITIONS

"AMSOL Associated Affiliates"	means all companies affiliated and associated to African Marine Solutions Group (Pty) Ltd [AMSOL].
"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 [AMSOL] including AMSOL Associated Affiliates.
"Data"	means "Personal Information" or "Special Personal Information".
"Data Subject" or "Data Subjects"	means the Company's employees, suppliers, contractors, agents' stakeholders and clients with whom it works.
"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.
"Person"	means a natural or juristic person.
"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.

"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 employees, suppliers, contractors, agents stakeholders and clients with whom it works in order to operate and to carry out its business effectively. POPIA imposes strict guidelines to secure a Data Subject's right to privacy with regard to their personal information, therefore, 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.

4. RIGHTS OF DATA SUJECTS

4.1 In terms of POPIA, Data Subjects have the following rights:

4.1.1 to be notified that personal information about him, her or it is being collected;

4.1.2 to be notified that personal information about him, her or it is being accessed or acquired by an unauthorised person;

4.1.3 to establish whether a responsible party holds personal information of that Data Subject and to request access to his, her or its personal information;

4.1.4 to request, where necessary, the correction, destruction or deletion of his, her, or its personal information;

4.1.5 to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information;

4.1.6 not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications;

4.1.7 not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person;

4.1.8 to submit a complaint to the Regulator regarding the alleged interference with the protection of Personal Information of any Data Subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator; and

4.1.9 to institute civil proceedings regarding the alleged interference with the protection of his, her or its Personal Information.

5. PROCESSING OF PERSONAL INFORMATION

5.1 The Company shall ensure that all Personal Information is processed lawfully and in a reasonable manner that does not infringe the privacy of the Data Subject.

5.2 Personal Information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

6. CONSENT

6.1 If consent is relied upon as required by POPIA for the purposes of processing, holding and/or the storage of any Personal Data, then such Personal Information may be processed, only if:

6.1.1 the Data Subject's consent has been obtained;

6.1.2 the Processing of the Personal Information is necessary for the conclusion or performance of a contract to which the Data Subject is a party;

6.1.3 the Processing complies with a legal obligation as imposed by laws on the Company;

6.1.4 the Processing protects a legitimate interest of the Data Subject;

6.1.5 the Processing is necessary for the proper performance of a public law duty by a public body; or

6.1.6 the Processing is necessary for the pursuance of a legitimate interest of the Company or a third party to whom the information is supplied.

6.2 With regards to Special Personal Information, the Company may only process such information under the following circumstances:

6.2.1 the Data Subject consents to such processing (Form 4 – Consent to be completed by a Data Subject for this purpose);

6.2.2 the Special Personal Information was deliberately made public by the Data Subject;

6.2.3 the Processing is necessary for the establishment of a right or defence in law; or

6.2.4 the Processing is required for historical, statistical, or research reasons. In the event that the Processing is in respect of race, gender, disability or ethnic original, then such Processing must comply with affirmative action laws.

6.3 All Data Subjects have the right to refuse or withdraw their consent to the Processing of their Personal Information and/or Special Personal Information, and a Data Subject may object, at any time, to the Processing of their Personal Information and/or Special Personal Information on any of the above grounds, unless legislation provides for such processing.

6.4 A Data Subject's withdrawal of consent to the Processing of their Personal Information must be reasonable when measured against the purpose for which the Personal Information is Processed. If the Data Subject withdraws consent or objects to Processing, and such withdrawal is reasonable, then the Company shall forthwith refrain from Processing the Personal Information and/or Special Personal Information. (Form 1 – Objection shall be used by a Data Subject for this purpose).

7. DATA RETENTION AND RESTRICTION

7.1 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.

7.2 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 will not apply to Personal Information that is retained by the Company if retention of such records are 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.

7.3 The Company may retain records of Personal Information for periods in excess of those contemplated in clause 7.2 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.

7.4 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 7.2 or 7.3 above. The record shall be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form.

7.5 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.

7.6 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.

8. FURTHER PROCESSING OF DATA

8.1 New processing activity must be compatible with the original purpose of processing. Any further processing will be regarded as compatible with the purpose of collection if:

8.1.1 the Data Subject has consented to the further processing of Personal Information;

8.1.2 the Personal Information is contained in a public record;

8.1.3 the Personal Information has been deliberately made public by the Data Subject;

8.1.4 further processing is necessary to maintain, comply with or exercise any law or legal right; or

8.1.5 further processing is necessary to prevent or mitigate a threat to public health or safety, or the life or health of the Data Subject or that of a third party.

9. NOTIFICATION OF DATA COLLECTION TO DATA SUBJECTS

9.1 When the Company collects any Personal Information, prior to such collection, it shall notify Data

Subjects of the following:

9.1.1 the purpose of which the Personal Information is being collected from the Data Subject;

9.1.2 whether the supply of the Personal Information by the Data Subject is voluntary or mandatory and the consequences of a failure to provide such information;

9.1.3 whether collection of the Personal Information is in terms of law authorising or requiring the collection of such information;

9.1.4 whether the Company intends to transfer the Personal Information to a third country or international organisation and the level of protection afforded to that information by that third country or international organisation; or

9.1.5 whether the Company intend to transfer the Personal Information to a third party.

9.2 If the Company has previously taken steps referred to under clause 10.1 below when it collected information from Data Subjects, it is not necessary for the Company to comply with the above, if the subsequent collection from the Data Subjects is the same information or information of the same kind if the purpose of collection of the information remains the same.

9.3 It is not necessary for the Company to comply with the sub-clause under clause 9.1 if the collection of information is to avoid prejudice to the maintenance of the law by an public body, to comply with an obligation imposed by law, to enforce legislation concerning the collection of revenue, for the conduct of proceedings in any court or tribunal, in the interests of national security or if compliance would prejudice a lawful purpose of the collection or it is not reasonably practicable in the circumstances of a particular case.

10. DATA SUBJECT'S ACCESS TO DATA

10.1 A Data Subject, with adequate proof of identity, shall have the right to:

10.1.1 request the Company to confirm that it holds Personal Information about it;

10.1.2 request from the Company a description of the Personal Information held by it or any third party.

10.2 All such requests shall be submitted in writing to the Information Officer. The Company may refuse, as the case may be, to disclose any information requested in terms of clause 10.1 on the following grounds of refusal:

10.2.1 the Company is protecting Personal Information about a third person (who is a natural person) including a deceased person, from unreasonable disclosure;

10.2.2 the Company is protecting Personal Information about a third party or the Company in respect of a trade secret, financial, commercial, scientific or technical information that may harm the commercial or financial interests of the Company and its affiliated companies or the interests of a third party;

10.2.3 if the disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement or contract;

10.2.4 if the disclosure of the record would endanger the life or physical safety of an individual;

10.2.5 if the disclosure of the record would prejudice or impair the security of property or means of transport;

10.2.6 if the disclosure of the record would prejudice or impair the protection of a person in accordance with a witness protection scheme;

10.2.7 if the disclosure of the record would prejudice or impair the protection of the safety of the public;

10.2.8 if the record is privileged from production in legal proceedings, unless the legal privilege has been waived;

10.2.9 if the disclosure of the record would put the Company at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;

10.2.10 the record is a computer programme; or

10.2.11 the record contains information about research being carried out or about to be carried out on behalf of a third party or the Company.

10.3 If the Company has searched for a record requested by a Data Subject (the "Requester") and it is believed that the record does not exist or cannot be found, the Requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken by the Company to try to locate the record.

11. RECTIFICATION AND CORRECTION OF DATA

11.1 The Data Subject may request the Company to rectify, correct or delete any Personal Information that is inaccurate, irrelevant, excessive, out of date, incomplete or obtained unlawfully. Form 2 – Correction shall be completed by a Data Subject for this purpose.

11.2 The Company must, within 30 (thirty) days of the Data Subject requesting the Company to either correct, destroy or delete the Personal Information, do so. The period can be extended to a further month, if the Data Subject's request is a complex request. The Company shall notify the Data Subject of the action taken as a result of the request and provide it with proof thereof.

11.3 In the event that the Personal Information has been disclosed to any third parties, the Data Subject must make the request to that party.

12. 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 either the loss of, damage to or unauthorised destruction of Personal Information or the unlawful access to or processing of Personal Information.

13. DATA PROTECTION MEASURES

13.1 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:

13.1.1 all emails containing Personal Information shall be encrypted using industry standard methods, if necessary;

13.1.2 all emails containing Personal Information must either be marked "confidential" or contain a disclaimer that the contents of the email are "confidential";

13.1.3 Personal Information may be transmitted over secure networks only;

13.1.4 all Personal Information which is transferred physically, including that on removable electronic media, shall be transferred in a suitable folder marked "Confidential";

13.1.5 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;

13.1.6 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;

13.1.7 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;

13.1.8 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;

13.1.9 all electronic copies of Personal Information should be stored securely using passwords and industry standard data encryption; and

13.1.10 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.

14. ORGANISATIONAL MEASURES

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

14.1.1 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;

14.1.2 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;

14.1.3 all employees, agents, contractors, or other parties working on behalf of the Company handling Personal Information will be appropriately trained to do so;

14.1.4 methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

14.1.5 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;

14.1.6 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;

14.1.7 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;

14.1.8 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.

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

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

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

15.2.1 is to a country that ensures an adequate level of protection for Personal Information;

15.2.2 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;

15.2.3 is made with the informed consent of the relevant Data Subjects;

15.2.4 is necessary for the performance of a contract between the Data Subject and the Company;

15.2.5 is necessary for important public interest reasons;

15.2.6 is necessary for the conduct of legal claims; or

15.2.7 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.

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

16.1 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) or data protection laws similar to those of POPIA, it shall ensure that it:

16.1.1 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;

16.1.2 obtains advice on the laws in that foreign country that permit access to Personal Information by government agencies; and

16.1.3 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).

17. DATA BREACH NOTIFICATION

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

17.2 If a breach of Personal Information occurs and that breach is likely to result in a risk to the rights and freedom 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;

17.3 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 17.2 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;

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

17.4.1 the details of the Data Subject which has been affected by the breach;

17.4.2 the nature of the Personal Information breached;

17.4.3 the likely consequences of the breach;

17.4.4 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

17.4.5 the notification shall be validated by the Information Officer.

18. DIRECT MARKETING

18.1 Direct marketing, including unsolicited direct electronic marketing is prohibited unless the Data

Subject has consented to the receipt of this marketing material.

18.2 In order to ensure that direct marketing is sent out in a lawful manner, all Personnel must ensure that:
- 18.2.1 all of the Company's clients, 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;
- 18.2.2 before direct marketing is sent to a non-client that such person provides his, her, or its consent thereto;
- 18.2.3 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
- 18.2.4 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.

19. REPORTING BREACHES OF PERSONAL INFORMATION

19.1 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.

19.2 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.

19.3 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 Information Officer with the approval of the Company's Board has the right to report any Personal Information or security breach to the Information Regulator and / or the affected Data Subjects, as the case may be.

20. ACCEPTANCE AND BINDING NATURE OF THIS DOCUMENT

20.1 By providing the Company with the Personal Information which it requires from a Data Subject, the Data Subject:
- 20.1.1 acknowledges that he/she understands why his/her Personal Information needs to be processed;
- 20.1.2 accepts the terms which will apply to such processing, including the terms applicable to the transfer of such Personal Information cross border;
- 20.1.3 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.

20.2 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.

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

20.4 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.

21. IMPLEMENTATION OF POLICY

This Policy shall be deemed to be effective as of 31 June 2021. No part of this Policy shall have a retroactive effect and will only apply to matter occurring on or after this date.

22. CONTACT

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