נתיבי הגז הטבעי לישראל
ISRAEL NATURAL GAS LINES

Ref: 473119

Privacy and Confidentiality Appendix

Whereas: Israel Natural Gas Lines Ltd. (hereinafter: "**the Client**") and _____ (hereinafter: "**the Vendor**") have entered into a Service Agreement between them, dated _____, according to which the Vendor will provide the Client with _____ services ("**the Services**" and "**the Service Agreement**", "**the Engagement**", respectively).

And whereas: And as part of the Engagement, the Vendor will carry out various activities on the Client's data bases, including processing data, direct access to information and/or he will hold the information.

And whereas: As part of the Engagement the Vendor might receive, or be exposed to, the Client's confidential information (as defined hereinafter) and/or personal information (as defined hereinafter, together with the confidential information, "**Information**").

And whereas: The manifestation of the Information, in its entirety or in part, and its disclosure to third parties might cause the Client considerable, serious damage, and so a condition for the disclosure of the Information, as stated above, is, inter alia, the Vendor's undertaking to maintain the confidentiality of the Information.

And whereas: The Information might contain, inter alia, Information that could be defined as "Inside Information" as defined in the Securities Law, 5728 – 1968 ("**the Securities Law**") and the use of which, or its transfer to others, might be an offense under the Securities Law.

And whereas: The Parties wish to define the areas of responsibility of each of the Parties to the Service Agreement, and to regulate the issue of the protection of the privacy of the Private Information, the data protection, the preservation of confidentiality of the Information and everything required to regulate the legal use of the Information.

And whereas: the Parties are interested in adding this Appendix to the Service Agreement, so that it will be an inseparable part thereof.

It is therefore agreed, declared and stipulated by the Parties, as follows:

1. General; Definitions

1.1. The introduction to this Appendix constitutes an inseparable part thereof. This Appendix constitutes an inseparable part of the Agreement, and all the provisions of the Agreement, as long as they have not been explicitly altered in this Appendix, will apply to the Appendix. In order to remove any doubt, the Parties declare that in any case of a conflict between the provisions of the Agreement and the provisions of this Appendix, the provisions of this Appendix will prevail.

1.2. The following terms are to be interpreted as follows:

1.2.1. "**The applicable privacy laws**" – the Privacy Protection Law, 5741 – 1981 ("**the Law**"), the regulations issued under it, including the Protection of Privacy Regulations (Information Security) 5777-2017 ("**Information Security Regulations**"), the Protection of Privacy Regulations (Transfer of Personal Information Outside the Borders), 5761-2001 (the "**Transfer of Personal Information Regulations Outside Israel**"), and the guidelines of the Privacy Protection Authority, including Directive of the Registrar of Databases No. 2/2011 entitled "Use of Outsourcing Services for the Processing of Personal Information".

1.2.2. "**Personal information**" – data about an individual that amounts to "Information" as defined in the Privacy Protection Law, and any other data about an identified or identifiable person, including information that identifies a person or can be used for identification, to locate a place or to contact a person. Personal information includes both information that directly identifies an individual such as a name, social security number or unique title, information that indirectly identifies an individual such as date of birth, mobile phone number, and also information that may lead to a particular person even if their identity is not easily and directly identifiable, such as IP address, statistics about website or software usage, including encrypted information, unless the processor does not have the key to the encryption.

1.2.3. "**Confidential Information**" - any information or data, whether written, oral or in any other form or means, belonging to the Client and/or relating to or associated with, directly or indirectly, the Client and/or his activity and/or information that has or will come to the attention of the Vendor and/or that has been provided or will be provided in any way, whether directly or indirectly, by the Client and/or by an executive or representative of the Client, including any know-how and/or idea and/or plan and/or commercial, financial, technical, business, economic and/or professional information relating to the Client and/or his activity and/or concern and/or objective, including information transferred as stated above prior to the date of signing this Agreement. Furthermore, confidential information shall be deemed the very existence of negotiations between the Parties to

enter into an agreement relating to the purpose. Notwithstanding the above, it is hereby made clear that the following information shall not be considered Confidential Information, provided that the Vendor has written proof thereof: (1) Information that is public knowledge at the time of this Agreement; and/or (2) Information that will become public knowledge in the future other than as a result of a violation of this Agreement; and/or (3) information that the Vendor already had at the time it was received; and/or (4) information provided to the Vendor by a third party who held the information without breaching its duty of confidentiality towards the Client; and/or (5) Information developed or prepared independently by the Vendor, not based on the Confidential Information and by persons who have not been exposed to the Confidential Information. The burden of proof that certain information meets one of the exceptions listed above will be on the Vendor.

2. Confidentiality

2.1. The Vendor undertakes to maintain absolute confidentiality over any Confidential Information that has reached and/or will reach it, and/or come to its knowledge, directly or indirectly during and/or in connection with the Service Agreement, and to take every reasonable step and precaution to safeguard such Confidential Information, including for the purpose of preventing the use of the Confidential Information not in accordance with the provisions of this Agreement, theft or loss.

2.2. Without prejudicing the generality of the above, the Vendor undertakes not to disclose, and/or transfer, and/or manifest, and/or pass on, and/or publish, and/or photograph, and/or copy, and/or duplicate, and/or remove from his possession (and/or to allow another or others to do so), the Confidential Information, or any part thereof, unless it is necessary to fulfill the objectives of the Engagement for which the information was given, and on a “need to know" basis.

2.3. The Vendor is aware that the Information is brought to its knowledge for the exclusive purpose of the Engagement, and not for any other purpose, and so, any use of the Information, or any part thereof, directly or indirectly, will be a violation of its undertakings under this Agreement, and the Vendor confirms that it is aware that the Information might contain information that might be defined as “Inside Information” as defined in the Securities Law, the use of which, and/or the transfer of which, might be an offense under the Securities Law.

2.4. The Vendor confirms that the Information that has or that will come into its possession or to its knowledge in any manner whatsoever, is the exclusive property of the Client, and the Vendor knows and agrees that: (a) the Confidential Information that has been disclosed by the Client is owned totally and exclusively by the Client, and it will remain his exclusive property, and its transfer to the Vendor does not constitute the granting of any rights to the Confidential

Information; and (b) the Confidential Information has been transferred and/or will be transferred as is, and without any obligation, representation or warranty on the part of the Client.

2.5. The Vendor undertakes that any employee, manager, consultant, vendor, subcontractor or executive of the Vendor, including in its subsidiaries or affiliated companies, to whom the information is about to be disclosed ("**authorized representatives and employees**") will be subject to the duty of confidentiality towards the recipient of the Information, the terms of which are not less than the terms of this Confidentiality Agreement and will not provide or disclose and/or permit access to Personal Information to any unauthorized third party. Without derogating from the aforesaid, the Vendor shall be responsible for the fact that authorized representatives and employees as stated above, act in accordance with the terms of this Agreement, and if any of the authorized representatives and employees and / or anyone acting on behalf of the Vendor who was exposed to the Information, does not fulfill the obligations specified in this section - it will be as if the Vendor breached its obligations under this Agreement.

2.6. The Vendor undertakes to return to the Client, at the end of the engagement, or immediately upon receipt of a first demand from anyone acting on behalf of the Client, whichever is earlier and at any time, any document or magnetic media or any other method of storage that contains Information, whether in writing or in any other form, that is and/or will be in the Vendor's possession at any time.

2.7. The Vendor is aware that transferring the Confidential Information and/or parts thereof and/or making any other use thereof, unnecessarily and to the extent necessary, may cause the Client heavy and irreversible damages, some of which are not pecuniary and therefore it is agreed that in any case of concern of a breach of this Agreement, the Client will be entitled, without derogating from any other remedy granted to him under this Agreement or under any law, to take action and issue injunctions and/or specific performance orders and/or any other temporary relief against the recipient of the information.

2.8. In the event that the Vendor is required by law to pass on the Confidential Information and/or any part thereof, pursuant to an order from a court and/or a competent authority, the Vendor undertakes, insofar as there is no legal impediment whatsoever, to notify the Client without delay of the requirement for disclosure soon after receiving it, and to the extent possible by law to allow the Client (insofar as this is under the control of the recipient of the information), reasonable time to act in order to prevent and/or minimize, as much as possible, the disclosure of confidential information. In any event, and without derogating from the above, the Vendor undertakes, as far as possible, to pass on only that part of the Confidential Information, the disclosure of which is required by law as stated above, to the extent and scope required of it.

2.9. The undertakings in this section shall remain in force indefinitely even after the conclusion or review of the engagement.

3. Protection of Personal Information

3.1. Processing Confidential Personal Information. The Parties recognize that the provision of the Services involves the Vendor processing Personal Information, including the Client's Confidential Information, including Personal Information on the Client's customers, his staff and his service providers. Therefore, the Vendor hereby declares that its undertakings concerning the protection of privacy and data security are the foundation for the Engagement between the Parties, and so, a substantial breach of any of the provisions of this Appendix, will be a fundamental breach of the Service Agreement.

3.2. Compliance with the legal requirements. The Parties acknowledge that the provision of the services entails, directly or indirectly, the Vendor's processing of Personal Information, including the Client's Confidential, including Personal Information of the Client's customers, employees and service providers. Moreover, the Vendor declares that it undertakes to comply with the obligatory requirements in the Service Agreement regarding the management of Personal Information and declares and undertakes that it complies and will continue to comply substantively throughout the entire period of the Engagement with the Client, with all the provisions of the applicable privacy laws regarding privacy protection, information security and the processing of Personal Information.

3.3. The objectives of the use: The Provider will process Personal Information on behalf of the Client for the limited purposes specified in Appendix A ("**Purposes of the Use of the Information**"). The Client hereby permits the Vendor to process Personal Information and Confidential Information for the purpose of providing the Services to the Client and in accordance with the purposes of using the Information, solely for the duration of the Agreement, and in accordance with the Client's instructions. The Vendor shall not process the Personal Information to which it will gain access for the Vendor's private purposes unless it has received the Client's express prior written consent.

3.4. Transfer of information outside of Israel. The Vendor undertakes that any transfer of Personal Information outside the borders of Israel, within the framework of this Engagement agreement and solely for the purposes specified therein, will be carried out in accordance with the Regulations for the Transfer of Personal Information outside of Israel, including and without derogating from the generality of the above, maintaining an adequate level of protection of the information at a level not less than that customary in Israel. If the Vendor makes use of the Information through sub-vendors outside of Israel, it will take care to store the information in accordance with the above.

3.5. Exercising privacy rights. The Vendor undertakes to act in accordance with the provisions of the applicable privacy laws and will ensure the realization of the privacy rights of the data subjects in connection with the Personal Information, including the right to review and correct the Information of the data subjects. In addition, the Vendor undertakes to ensure that any inquiry from the subject of Information on such a matter is immediately brought to the attention of the Client and the Vendor will act in accordance with the Client's instructions.

3.6. Registration as a "holder". If the Vendor's activity vis-à-vis the Client amounts to a "holder" of a database as defined by law, then the Vendor undertakes to act in accordance with the requirements of the applicable privacy laws, and to cooperate with the Client for the purpose of registering him as a holder in the Registrar of Databases.

3.7. Duration of information retention. If the Client's Personal Information is stored in systems owned by the Vendor, the Vendor undertakes to retain the Information only for the time required to carry out the services, and subject to the Client's written request to destroy any information that is no longer necessary for the purpose of providing the services to the Client or at the end of use, in accordance with this Agreement below, except for Information that the Vendor is obligated to keep by law, Information that is stored for the purpose of documenting and archiving the service to the Client or for legal proceedings – and in each of the cases listed above, the Vendor will restrict access to the Client's Personal Information only for these needs.

4. Data security

4.1. The Vendor will sign a data security appendix which will constitute an inseparable part of this Appendix and the Service Agreement (Appendix B – Data Security).

5. Infrastructure security

5.1. Furthermore, the Vendor undertakes to maintain the confidentiality and security of all the authorizations and passwords associated with the service and also to implement any other operational or technical security measures to protect the service from illegal access or use. The Vendor shall be responsible for any consequences that may arise from unauthorized access or illegal use of the Confidential Information and/or the Personal Information.

5.2. The Vendor will verify that it only uses supported versions of operating systems, browsers, databases and software infrastructures. It is made clear that systems whose security aspects are not supported by the manufacturer will not be used unless an appropriate security response is provided.

5.3. The Vendor will protect the database and toughen it by using accepted encryption methods.

5.4. Any change to the database will be made in coordination with the Client regarding the type and nature of the required change and documentation of the changed values. The Vendor will provide the Client with maximum availability of the services during operating hours and will operate a DDOS mechanism to prevent downtime.

6. Management and control

6.1. The Vendor will place at the Client's disposal all the information required to prove its compliance with its obligations under the Service Agreement and this Appendix, including authorization and/or reasonable assistance to carry out control and inspection of the Vendor to be carried out by the Client or anyone acting on his behalf. Including, without derogating from the generality of the above, receipt of regular reports and documents pertaining to the manner in which the Client's Personal Information is managed, and compliance with its obligations in connection with the performance of the services.

6.2. During the entire period of the Engagement agreement, the Client will be entitled to carry out monitoring, regular checks and surprise checks, of the Vendor's activity with regard to the execution of the Engagement agreement. The Vendor undertakes to handle all findings and defects (if discovered) presented to him by the Client, at the expense of the Vendor, in accordance with the Client's instructions.

6.3. The Vendor shall inform the Client of the geographical location of the place where the Personal Information is physically stored or processed by the Vendor or its authorized subcontractors, including the transfer of information outside the borders of Israel and any changes to such location.

7. Engagement with subcontractors

7.1. The Vendor shall be entitled to provide some of the services through subcontractors as specified in Appendix A, provided that it enters into contracts with any subcontractor as stated in the agreement regulating the matters specified in this Appendix. It is made clear that the Vendor shall bear legal responsibility for any act or omission on the part of a subcontractor on its behalf within the framework of the Services.

7.2. Prior to the Vendor's engagement with subcontractors or other third parties that were not known to the Client at the time of signing the Services Agreement, the Vendor shall obtain the Client's consent for the purpose of processing the Client's Personal and/or Confidential Information.

7.3. It is the responsibility of the Vendor to conduct a risk survey and due diligence with respect to the reliability of the sub-Vendor and its ability to comply with the terms of this Appendix, to ensure that there is no other risk of improper use of the Information by the sub-Vendor, and to document this process.

8. Reports

8.1. The Client will be entitled, at his reasonable request at any time, to receive regular reports from the Vendor on all matters associated with the management of the Client's Personal Information, the database involved and the processing of the above-mentioned Information.

8.2. Without derogating from the generality of the above, the Vendor undertakes to give the Client an annual, written report, at a level of detail that will satisfy the Client, which will specify the manner of compliance with its obligations with respect to the Protection of Privacy Law and aspects of information security in connection with the performance of the services and this Appendix. In addition, the Client is entitled to demand additional detail for the report and also supporting documents.

8.3. The Vendor shall immediately notify the Client of any unauthorized use or disclosure of personal or confidential Information, and/or any security incident (whether serious or not), or any suspicion of a security incident in its information systems, including and without derogating from the generality of the above, when the Vendor believes that unauthorized use or disclosure of Personal or Confidential Information has been made. The Vendor shall immediately take, at its own expense, all necessary steps to correct the deficiencies and prevent the recurrence of such incidents. Furthermore, the Vendor undertakes to cooperate reasonably with the Client in order to comply with the requirements of the law regarding security incidents, if any, including to the extent that it is required to provide notice about an event, as mentioned above, to anyone who may be affected by it, subject to the requirements of the law. Insofar as the Vendor is required to report to a competent authority regarding the security incident, the Vendor undertakes to update the Client before doing so and will coordinate with him, to the extent permitted by law.

9. The Vendor's responsibility

9.1. Notwithstanding the contents of the Service Agreement, the Vendor declares and undertakes that it is responsible for any damage caused to the Client in association with its non-compliance with this Appendix, including and without derogating, in association with any information security incident, any incident of leakage of information, and/or unauthorized use of information, and/or any other matter as stated in this Appendix.

9.2. Notwithstanding the contents of the Service Agreement, to the extent that is stated, the Vendor will indemnify the Client, on his first request, in association with any damage that will be caused to the Client in association with a substantial breach of the provisions of the applicable privacy laws, and in association with any damages that will be caused as a result of an information security incident (whether serious or not).

9.3. This undertaking does not derogate from any obligation of ours, under any law, in association with loyalty and maintaining confidentiality, and it comes to supplement them and not to detract therefrom.

10. Termination of the engagement between the two parties

10.1. The length of the engagement between the Parties has been set in the Service Agreement. This Agreement will be valid for the entire period of the engagement between the Parties.

10.2. In any event of the termination of the Service Agreement, the Vendor will take immediate action to delete all the Client's Confidential Information and Personal Information; or, alternatively, in the event that the Client makes a written request, the Vendor will take action for the immediate transfer of the aforementioned Confidential Information to the Client, and in coordination with him. This includes the entire up-to-date data base, including products prepared using the Information while providing the services, starting from the date of the commencement of the provision of the services. Thereafter the Vendor will give written confirmation, signed by an executive of the Vendor, of the deletion or transfer of the aforementioned Information. The Vendor will cease to provide the services, and will also block any access by him, and/or anyone acting on his behalf, to the Client's Personal Information, and/or Confidential Information.

11. General

11.1. As long as the Vendor processes the Client's Personal Information and/or Confidential Information, the Vendor's obligations, set forth in this Appendix, regarding the protection of privacy and confidentiality will continue to apply even after the termination of the Service Agreement and the termination of this Appendix, for any reason whatsoever, unless the information is kept anonymous, after the characteristics of the subjects of the data have been finally and immutably removed, and subject to the delivery of an undertaking by an executive of the Vendor in this regard.

11.2. In the event that any of the undertakings set forth in this Appendix are declared null or unenforceable, it shall not prejudice the remaining undertakings under this Appendix which shall remain in force. Furthermore, if such an undertaking is found to be null or unenforceable only because of its scope or period or such limitations, then the Parties agree that such an undertaking shall be qualified by the competent court so that it will be enforceable to the maximum extent and period permitted by law.

We have come to sign:

_____	_____	_____	_____
Name	**Company name**	**Date**	**Signature**

Appendix A – Information Processing

a. <u>Types of Information that the Vendor will process</u>

For example: contact information / demographic information / consumption habits / behavior habits / political opinions / audio or video recordings / economic information - debts / economic information - assets / biometric information / genetic information / medical information / religious affiliation / mental state / sexual orientation / professional experience / education / communication data other than contact details / criminal history / family ties / family tree / sensitive other (sensitive)_____ (*specify)* other non-sensitive_____ -

b. **<u>The objectives of the usage that are permitted for the purposes of the Agreement</u>**:

The use and processing of the Personal Information is limited to the sole purpose of providing the services, as specified in the Service Agreement, only as long as the Service Agreement will remain valid and the services are provided by the Vendor to the Client, including the support and maintenance period.

c. <u>Types of Information Subjects (those about whom there are Personal Information records)</u>

For example: The company's employees, contractors and the company's service providers, customers, vendors.

d. **<u>The Vendor's sub-contractors who have access to the Personal Information</u>**:
(Please complete)

Name of sub-contractor	Type of services	Location where information is stored

Completed by:
Position:
Date:

Appendix B – Information Security

1. Definitions

1.1. **Information Security** - all the actions and the measures required to ensure that the integrity, availability, reliability, confidentiality and survivability of information assets are maintained.

1.2. **Information Asset** - a file, record, database or physical copy, containing information created or received as part of the company's ongoing activity, and of value to the proper functioning of INGL.

1.3. **INGL's Information Environment (at the Vendor)** – INGL's information assets and all the infrastructure, and components that enable access to them, or in which they are created, maintained, processed or transferred.

1.4. **Confidentiality** – a requirement that access to information be limited only to parties defined as requiring this access, and to whom permission has been granted accordingly.

1.5. **The Confidential Information** – Information received by the Vendor and/or those acting on his behalf for whom access has been authorized ("**Authorized Access**"). Authorization to hold, process or authorization to access in accordance with the provisions of this Appendix, as set forth in Section **שגיאה! מקור ההפניה לא נמצא.**, below.

1.6. **Information Security Incident** – Information exposed to unauthorized parties that may endanger the organization, violate the privacy of its employees and contractors, harm INGL's business activity or constitute a violation of the law of any kind.

2. General guidelines

2.1. As part of the implementation of its obligations to INGL, as specified in the agreement between the Parties, the Vendor is hereby granted limited, temporary authorization to hold and process, for INGL, the Confidential Information set forth below:

Type of Information for which the Vendor is authorized to process	**Permitted type of process or action**	**Purpose of the processing or permitted action**	**The system which the Vendor is authorized to access**

As part of the implementation of its obligations to INGL, as specified in the agreement between the Parties, the Vendor is hereby granted, through those

with authorized access, limited, temporary authorization to receive access to INGL's Information, and/or to the INGL systems only as specified below:

Type of Information for which the Vendor is authorized to access	**Permitted type of process or action**	**Purpose of the processing or permitted action**	**The system which the Vendor is authorized to access**

In order to avoid any doubt, the vendor will not process, hold or try to receive access, or to view any Information or system that is not of the type specified above, unless subject to the approval of INGL.

2.2. The Vendor undertakes not to process any type of Confidential Information, other than for the purposes specified in this document and in the manner specified in this document. In the event that any Information that is not of the type specified in this document comes to the vendor's knowledge or possession, the Vendor will inform INGL immediately and will act according to INGL's directives.

2.3. The Vendor undertakes that he and those authorized and acting on his behalf will act according to the INGL directives, or the directives of someone acting on its behalf, as will be from time to time, with regard to the use and processing of confidential information, provided that the instructions were provided to the Vendor in advance and in writing.

2.4. The Vendor hereby declares and undertakes that he and/or those authorized to access on his behalf will not make any use of the Confidential Information except for the purpose of performing the Vendor's obligations towards INGL as part of the contract between the Parties. The Vendor will be solely responsible for any use made by those authorized to access the Confidential Information and will be responsible for preventing the leakage of INGL's Information to unauthorized parties.

2.5. The storage of confidential information on the Vendor's sites and/or systems and/or infrastructures will be carried out securely and in accordance with INGL's information security guidelines as updated from time to time, subject to regulatory and technological changes and various information security threats. Without derogating from the above, the Vendor shall keep the Confidential Information separate (by means of logical separation such as separation of folders) from any other information available to the Vendor, including information belonging to the Vendor's other clients.

2.6. In order to remove any doubt, it is made clear that this document includes both general provisions that are binding on the Vendor in every case, and also concrete provisions that regulate specific cases, compliance with which is binding only subject to the specific case being included in the

framework provided in accordance with the Agreement. Thus, for example, guidelines regarding safe use of Wi-Fi will be binding in a situation where Wi-Fi is used by the Vendor on a network containing INGL's Confidential Information, and instructions regarding cloud storage will be relevant if the contract includes storing Confidential Information on a cloud.

2.7. The Vendor shall appoint a contact person, on its behalf, who will be responsible for Information Security matters with regard to the systems provided by the Vendor or the services provided by the Vendor to INGL, and for the implementation of all the requirements specified in this document. The above-mentioned contact person shall be available on an ongoing basis to the Information Security and Cyber Protection Manager at INGL, in order to respond to inquiries regarding the matters set forth in this document.

2.8. Once a year, the Vendor must conduct a self-security survey in accordance with the Cyber Directorate's methodology regarding the supply chain, and it must correct any material findings that arise in it.

2.9. The Vendor will perform resilience tests, through an independent party, of INGL's Information Environment infrastructure, at least once every 18 months, or with any significant change in the network. The Vendor will update INGL with the critical findings and will take care to address them within a reasonable time.

2.10. The Vendor's obligations to make the Information secure as stated in this Information Security Appendix are a fundamental condition for INGL's engagement with the Vendor.

2.11. The Vendor declares and undertakes that it will adopt all Information Security measures accepted in the industry in order to ensure the integrity, availability, confidentiality, survivability and reliability of the Information, including measures to prevent leakage of the Information – whether it is Information stored and/or processed in the Vendor's database systems or when transferring the information from INGL to the Vendor and/or from the Vendor to INGL and/or from the Vendor to a third party.

2.12. All the provisions of this Appendix, with the required changes, will apply to any Information to which the Vendor and those with access authorization will be disclosed during the provision of the service to INGL. Without derogating from the above, it is made clear that the Vendor and those with access authorization are not authorized to make any use of Information for which authorization has not been granted as stated in section **שגיאה! מקור ההפניה לא נמצא.** above.

3. Reports

3.1. The Vendor undertakes to inform the Information Security and Cyber Protection Manager at INGL immediately that he becomes aware of any Information Security Incident, or any suspicion of an Information Security incident that affects or might affect the INGL Information Environment, and he will provide INGL with all necessary assistance in the matter. An Information Security incident includes, inter alia (but is not limited to) hacking systems, spreading a virus / malware, unauthorized access to information or information systems containing information, leakage of information (malicious or accidental), etc. The Vendor shall investigate any such incident, report to INGL on the weaknesses discovered in the services or the systems it provided as part of the investigation and shall update INGL on the measures it has taken to correct them.

3.2. The Vendor undertakes to report to the Information Security and Cyber Protection Manager at INGL any suspicion that has come to its attention regarding the presence of a malicious code, virus, Trojan horse, etc. in relation to the system provided by the Vendor to INGL (if such a system was provided).

4. Compliance with regulations, standards and procedures

4.1. The Vendor shall determine and implement in its organization, at all times, an updated and valid Information Security policy and procedures, in accordance with the relevant regulations and legal requirements, including the methodology of the Cyber Directorate regarding the supply chain, as updated from time to time, in accordance with the service it provides, which will be available and binding in relation to the Vendor's people with access authorization. Information security procedures shall relate, inter alia, to the following issues: (a) physical security;(b) logical security; (c) separation of information; (d) policy regarding termination of use of information and removal of information storage equipment; (e) processes related to the sorting of information;(f) accessibility of control; (g) confidentiality obligations of authorized persons; (h) auditing; (i) recruitment and training of employees and conducting background checks (inter alia, regarding the training of employees authorized to access INGL's Information Environment for Information Security issues in general, and the risks relevant to the performance of their duties in particular), subject to the limitations of the relevant laws (for example, Israel Police Directives 151, a certificate of integrity, internal background checks of

INGL or any other check approved by the law authorities); and (j) Compliance with additional Information Security instructions.

INGL will be entitled to request from the Vendor at any time a copy of these procedures.

4.2. If the Vendor has access to information on system infrastructures, the Vendor undertakes that it is certified to an international standard for information security management – ISO27001 and will continue to hold this certification as long as it has such access. The Vendor undertakes to provide INGL with a photocopy / scan of a valid certificate of accreditation as part of the signing of the Agreement, and as part of any update or renewal of the aforementioned accreditation certificate.

4.3. In the event that the Confidential Information contains Information about people, the vendor will act entirely in accordance with the Protection of Privacy Law, 5741-1981, and the regulations enacted pursuant thereto, and any relevant directive of the Privacy Protection Authority at the Ministry of Justice (hereinafter, collectively: the "Law"), including the Protection of Privacy Regulations (Data Security), 5777-2017, as if it were the "holder" of the information for INGL in accordance with the Law. If, at INGL's discretion, the Vendor must be registered as the "holder" of INGL's databases in accordance with the provisions of the Law, the Vendor will cooperate with INGL and provide it with all the information required in this regard.

4.4. The Vendor shall not store information in systems located outside of Israel, except with the Vendor’s prior written approval. Without derogating from the above, in any case of storing information outside of Israel, the Vendor will store information only in a member state of the European Union and subject to the GDPR regulation and subject to compliance with the Protection of Privacy Regulations (Transfer of Information to Databases Outside the Borders of the State of Israel), 5761-2001.

4.5. The Vendor shall provide INGL, at its request, no more than once a year, with a report on the manner in which the Vendor has met its obligations under this Information Security Appendix and the provisions of the applicable law.

5. Collection and transfer of Information, and cooperation with third parties

5.1. If, as part of the services that it supplies to INGL, the Vendor is required to collect information from a person and to manage it as part of the Confidential Information, the Vendor hereby declares and undertakes that any request to a person for Information for the purpose of holding or using it as

part of the Confidential Information, whether it is carried out by the Vendor or by anyone acting on his behalf, will be accompanied by advance notice with the following be specified therein:

5.1.1. Whether that person has a legal obligation to provide the Information, or the disclosure of the Information depends on his good will and consent.

5.1.2. The purpose for which the Information is sought.

5.1.3. To whom the Information will be provided and the purposes of its transfer.

The wording of such a notice on behalf of the Vendor shall be submitted in advance for approval by INGL.

5.2. The Vendor hereby declares and undertakes that it will not collect Information in illegal ways, and will not make use of, or combine the Confidential Information with Information from illegal databases or illegal information that has reached it.

5.3. Files containing INGL's Confidential Information will be transferred only in encrypted form. Files containing Confidential Information may not be transferred by email and/or by any other means of communication to other parties without INGL's prior written permission.

5.4. The Vendor undertakes that any engagement it has with a sub-Vendor that receives access to Confidential Information will be made only subject to INGL approval of the identity of such a subcontractor. If INGL approves the use of a sub-Vendor as stated above, the Vendor undertakes to include appropriate clauses that impose on the sub-Vendor confidentiality and Information Security obligations identical to those imposed on the Vendor under this Information Security Appendix, provided that in any case such clauses include – (1) the provisions required by the Law;(2) provisions prohibiting the transfer of information to additional third parties;(3) provisions ensuring that the sub-Vendor takes sufficient measures to ensure the privacy of the persons that are the subjects of the Information, taking into account the scope of the Information disclosed to the sub-Vendor, its sensitivity and the other relevant circumstances.

6. Security of the network on which the Information is stored

6.1. General

6.1.1. In a situation where Information is stored or processed for INGL, the servers or computers that contain the above-mentioned Information will not be connected directly to the internet nor to external networks and will not be stored on a server directly accessible from the internet (a DMZ server on a network directly facing the internet). Any deviation from this condition requires the prior approval of the Information Security and Cyber Protection Manager at INGL.

6.1.2. Digital Information that is classified as confidential shall not be transferred by means of the internet, or by regular email, between the vendor and INGL, or between the Vendor and sub-vendors, but only on a secure channel that will be given at the time of the transfer by the Vendor's contact person at INGL.

6.2. Storage of information

6.2.1. In cases when INGL's Confidential Information needs to be kept on a laptop or on removable media, the files, the removable media or the computer's hard drive must be encrypted.

6.2.2. The Vendor shall implement internal compartmentalization in access to files containing Confidential Information in relation to those with access authorization its behalf. Access to these files will be possible only for those whose work and position with the Vendor require it, and to those who have signed a confidentiality undertaking. The Vendor shall maintain an updated record of those persons with access authorization, for whom access is required in order to perform the Vendor's obligations, the type of access authorization granted to them and the purpose for which access is required.

6.2.3. Magnetic or optical media will be stored, in coordination with INGL, in a place to which access will be possible only for those with access authorization.

6.2.4. Backups will be carried out in an orderly manner and will be kept in a closed and locked place with access to the person responsible for the backups only. The Vendor must also maintain a periodic restore procedure for backups.

6.2.5. It is forbidden to transfer tapes or other removable media with backups of files containing Confidential Information to external parties without prior notice and receiving INGL's approval.

6.2.6. Any magnetic or optical media or report that constitute processing products from INGL data will be stored in a locked cabinet and will be destroyed and shredded after use.

6.3. Workstations

6.3.1. INGL's files will not be saved on the station's hard disk (except for a company or individual without a user network).

6.3.2. Entry to the station will be by means of a user ID and individual password.

6.3.3. The length of the password will be at least eight characters.

6.3.4. The passwords will be changed at least every three months.

6.3.5. A user who fails five times in succession when trying to identify himself will be automatically locked out.

6.3.6. Enforcement is required that locks the organization's computers after 20 minutes without the computer being used.

6.3.7. All Microsoft operating systems will have software installed to prevent hostile EDR code + antivirus.

6.3.8. Critical information security updates will be performed on all operating systems at least once a quarter.

6.3.9. Removing a hard disk from the Vendor's servers or personal computers (except for a company or individual without a user network) for repair or for any other purpose, when there are files on them that contain Confidential Information, is prohibited. In such a case, the information shall be deleted, and the disk formatted.

6.4. Using wireless networks

6.4.1. Wi-Fi communication will be performed using the latest and most secure security protocol.

6.4.2. Public Wi-Fi networks are not to be used.

6.5. Remote access on the Vendor's network

6.5.1. INGL's Information Environment will be remotely accessed, based on at least the following security settings:

6.5.1.1. Defining a multi-factor authentication (MFA) on access to the service.

6.5.1.2. A full event log will be defined on the use of the service.

6.5.1.3. Access to the service and traffic will be encrypted based on market standards.

7. Laptops and Mobile

In the event that during the provision of the services to INGL, the Vendor will hold Confidential Information on mobile computers (e.g. disk on key, laptop, mobile phone, tablet), the person with access authorization must act as follows:

7.1. The mobile device will be under the supervision of the person with access authorization at all times. If the person with access authorization does not take the mobile computer device with him, for any reason whatsoever, he must lock it in a safe place.

7.2. If the mobile device is lost, the person with access authorization or the Vendor's contact person must report the loss, immediately, to the Information Security and Cyber Protection Manager at INGL, and/or the Security Officer, and he must specify the type of Information that was on the computer device that was lost, and how it was protected and backed up.

7.3. If files containing Information on customers and/or details of INGL's systems, are used, the Vendor must ensure that these documents are encrypted individually, and/or each memory device will be encrypted.

7.4. As a rule, memory devices, with files on them that contain INGL Information, will not be removed from the mobile computer devices for repair, or for any other purpose. If such an action is perpetrated, the user must delete the Information and format the disk.

8. Security of Information on a Cloud

Without derogating from the rest of the provisions in this Appendix, if, during the provision of services to INGL, as specified in the contract between the Parties, INGL's Confidential Information will be held on cloud infrastructure, the Vendor is obligated to act and/or to cause his cloud service vendor (if a third-party cloud service vendor is employed) [to act] as follows:

8.1. Confidential data will only be held on servers located in the EU Region.

8.2. A contact person will be defined at the cloud service vendor for information security issues (audits and events), who will be available for INGL's inquiries.

8.3. Reports on Information Security on cloud incidents will be sent to INGL, as specified in section **שגיאה! מקור ההפניה לא נמצא.שגיאה! מקור ההפניה לא נמצא.**, above.

8.4. The cloud vendor will be responsible for implementing mechanisms, procedures and work processes that will enable continued business activity and continued access to Confidential Information by INGL, even during an Information Security incident.

8.5. INGL will be notified of any demand by the authorities to provide / review the Confidential Information, and INGL will be allowed to defend itself, or restrict this access vis-à-vis the relevant authority, at its discretion.

8.6. The cloud Vendor shall notify INGL of any change in the ownership of the cloud vendor and shall ensure that any such change is made only subject to the purchaser assuming all obligations of the seller.

8.7. The Vendor's cloud vendor shall constitute a subcontractor for all intents and purposes, including for the purposes of the section 5.4 above.

8.8. INGL will be entitled to perform audits and penetration tests for the cloud service, including performing a physical audit at the Vendor's site by Information Security representatives and INGL's security unit. If necessary, the Vendor will be able to choose a third-party vendor agreed upon by INGL to perform the tests on its behalf. The inspection report will be sent to INGL.

8.9. Switching to cloud storage or changing the method of cloud storage will be subject to prior written approval, including after INGL has made all the necessary decisions in this regard.

8.10. The cloud service must comply with INGL's relevant regulatory rules and standards in accordance with ISO-27001 and/or ISO-27017 standards, and the provisions of any law.

8.11. INGL data will be deleted from the computer devices used by the Vendor after the end of their use or at the end of the service, whichever comes first.

8.12. The Vendor will ensure encryption of files containing INGL's Confidential Information with the latest and most secure protocol.

8.13. If necessary, the organization will be able to erase the Information from the cloud service completely.

9. Those with authorized access and instructions for receiving access to the systems

9.1. The Vendor will be responsible for granting access to the Information to those authorized to access the Information only after checking and verifying, by reasonable means customary in employee screening and placement procedures, that there is no concern that the person with authorized access, who receives authorization, is not suitable for obtaining access to the Information, taking into account the sensitivity of the Information and the scope of the authorization granted to that authorized person.

9.2. The Vendor undertakes that those authorized to access the Information will implement all the security measures set forth in this Information Security Appendix.

9.3. The Vendor shall implement internal security and the monitoring of measures through which it will ensure that any access to the Information is made solely by the authorized persons and solely for the purpose of performing the Vendor's obligations towards INGL. The Vendor will instruct those with authorized access on its behalf about the conduct required with regard to the Information, in accordance with the provisions set forth in this Appendix.

9.4. If, as part of the provision of services to INGL, personal identification and connection details to INGL's networks and/or systems are allocated to the Vendor’s persons with authorized access, the Vendor will be responsible for those with authorized access acting in accordance with the instructions set forth below, from any site and connection point from which connection will be made to the INGL systems, including the Vendor's systems or personal endpoints of those with authorized access:

9.4.1. If a username and password have been defined for that person with access, for him to authenticate the identification information vis-à-vis the information systems - the password is personal and confidential. Do not pass on the password to anyone, including the Vendor’s employees. If a password and username other than his/her own are provided to a functionary, it is strictly forbidden to use them.

9.4.2. The Vendor will notify INGL immediately of the long-term absence of any person with authorized access (including in the case of recruitment, unpaid leave, maternity leave, mobility and leaving).

9.4.3. Do not register your username and password in a visible place. If necessary, secure storage should be used - storage in a physical paper safe and use of encryption for a computer file.

9.4.4. It is forbidden to make any changes to the endpoints from which the connection was made, including through the installation of software.

9.4.5. If the person with authorized access suspects unauthorized use of his login details or the endpoint from which he connects, he must report it immediately to INGL's Information Security and Cyber Protection Department.

9.5. A person with authorized access who leaves an end station, from which a connection to INGL systems has been made, must ensure that the end station is locked, in such a way that it will not allow further work on the INGL systems without reconnection.

9.6. Do not connect external devices such as USB drives, modems, media players, etc. to the endpoint from which connection to INGL has been made, as well as any other means that use a wireless communication medium (Bluetooth, Wireless, Infrared) and more.

9.7. It is strictly forbidden for those with authorized access to save files locally on the end stations.

9.8. The Vendor undertakes to hold, from time to time, and in any case at least once a year, training for those with authorized access the information regarding their obligations to maintain Information Security (including in accordance with the provisions of this Information Security Appendix) and the applicable law. The Vendor undertakes to grant authorization for access to the Information subject to the holding of such training, while for a new person with authorized access – such training will be conducted as close as possible to the date of commencement of his work or, as the case may be, his accreditation. The Vendor undertakes to keep documentation for performing such training and will provide INGL with this documentation, at the latter's request.

9.9. The Vendor will verify the revocation of authorization and the return of equipment and information platforms containing INGL information, when an employee leaves or changes his position, and will update the party at INGL with whom he works.

9.10. The Vendor undertakes to document all activity carried out in the Vendor's systems, including, but not limited to, documentation of attempts to

access the Vendor's systems, deletion and/or change of information, development activities in the Vendor's systems and change of access authorization to the Vendor's systems (the "Documentation Mechanism"). The documentation mechanism will collect at least the following data: the identity of the user, the date and time of the operation, the source of the operation (Internet address or computer name), the system component in which the operation was performed, the type of operation and whether the operation succeeded or failed. The documentation data produced by the documentation mechanism will be retained throughout the term of the Agreement, unless INGL instructs otherwise in writing. The documentation mechanism will not allow, to the best of its ability, cancellation or modification of its operation, it will detect modifications or cancellations in its operation and will send alerts to those responsible. The Vendor shall establish a routine examination procedure for data generated by the documentation mechanism and shall draw up a report of the problems discovered, and measures taken as a result.

10. Security of physical documents

10.1. Documents and/or files and/or any hard copy material that was removed from INGL for work purposes will be returned to the party with whom INGL is contracted for shredding or destruction immediately upon completion of their processing.

10.2. Documents containing INGL Information will be kept locked in a locker, drawer, cabinet or safe allocated for this purpose only.

10.3. Access to these documents will be permitted only for those whose work and position with the Vendor require it, and to those who have signed an undertaking to maintain confidentiality with INGL.

10.4. It is forbidden to transfer documents containing INGL printed material to other parties by any means (fax, Israel Post, etc.) without written permission from INGL.

10.5. Do not leave documents with INGL material on the desk/printer at the end of the working day.

10.6. Documents containing INGL Information must be shredded at the end of their use.

11. Audits and risk reviews

11.1. The Vendor undertakes to allow INGL or anyone acting on its behalf to carry out Vendor audits and Information Security audits on its premises. The checks will be carried out during the Vendor's normal operating hours and in coordination with him, a reasonable time in advance, provided that during or near an Information Security event (as specified in section **שגיאה! מקור ההפניה לא נמצא.**) the audits may be carried out outside of normal operating hours but at reasonable dates and times under the circumstances.

11.2. These audits will examine the Vendor's compliance with the provisions of the applicable law and INGL's guidelines (including the guidelines set forth in this Information Security Appendix), including the following aspects:

11.2.1. The use and security of INGL information.

11.2.2. That there is no transfer of information to and from the Vendor's premises and to third parties.

11.2.3. That there is no retention of information at the Vendor.

11.2.4. An examination of technological information security controls, including an examination of the definitions of communication components, information security and servers.

This is in order to ensure that the Information Security guidelines as specified in this document are implemented.

11.3. Without derogating from the above, in order to carry out audit and supervision activities of the Vendor's Information Security activities and its compliance with the Information Security requirements, according to this Appendix and the applicable law, INGL will be entitled, at its exclusive discretion, to require the Vendor to fill out information disclosure questionnaires and risk surveys, to the extent reasonably required, including, but not limited to, as required in accordance with the guidelines and circulars of the Ministry of Health and/or the Privacy Protection Authority, as they will be from time to time.

11.4. The Vendor shall conduct, at least once every 18 months, a risk survey to identify Information Security risks and penetration tests to its Information Systems that store Information and/or from which INGL's information systems can be accessed. The Vendor will discuss the results of the risk survey and penetration tests with INGL, it will examine the need to update its security

procedures as a result and will act to correct the deficiencies discovered in the survey and tests, if any are discovered, without delay. The Vendor will provide INGL with confirmation that such surveys and audits have been conducted and that the deficiencies, if any are discovered, have been corrected.

12. The period of the engagement and the return of the Information

12.1. The Vendor undertakes that immediately on the termination of the engagement with INGL, for any reason whatsoever, or immediately on INGL's first written demand, he and his persons with authorized access will (a) cease to make any use of the Confidential Information. (b) will return and/or destroy all the Confidential Information and any copy thereof that they have. (c) Will give the person at INGL with who they worked, a declaration, signed by a senior executive of the vendor, confirming that all the Information has been returned or destroyed, as stated above, including magnetic Information or Information on systems in the Vendor's possession.

_____ _____

Signature and stamp Date