Part B -
Engagement agreement

Table of contents

Engagement Agreement for International Public Tender No. 110-2024 on the Subject of –

procurement, adjustment, testing, installation, instructing on, deployment and maintenance of LIMS laboratory management system at governmental medical centers

drafted and signed on the ____ of the month of _____ 2024

Between

The Government of Israel on behalf of the State of Israel, which is represented for the purposes of this Agreement by the Director General of the Ministry of Health, or the Deputy Director General at the Ministry of Health, together with the accountant of the Government Medical Centers Division at the Ministry of Health or their deputy, who are authorized to sign on its behalf according to the authorizations published in the Publications Satchel of Israel.

(hereinafter: the "**Division**" or " **Client**")

Of the first part

and

The winner _____ Identifier (Private Company / Identity No.) _____
whose address is _____
through the winners authorized signatory whose signature binds it

(hereinafter: the "**Supplier**")

Of the second part

Whereas: The Division published the tender in the title and relying on the statements in the Suppliers tender bid, the Supplier has been confirmed as the winner by the automatic data processing tenders committee of the Division; and

Whereas: The Supplier declares that it owns all rights required by statute to execute this Agreement and that there is no impediment, statutory and/or contractual and/or otherwise, to its engagement with the Division to execute this Agreement in its entirety; and

Whereas: The Supplier declares that the fulfillment of its obligations towards the Division, as set forth in the tender documents and herein, does not constitute any infringement of proprietary rights of another person and/or entity, including infringement of copyright and patent rights; and

Whereas: The represents and warrants towards the Division that it and its delegates have the ability, know-how, expertise and means required for providing the services set forth in the tender and herein (the "**Services**"); and

Whereas: The Division is interested in receiving the services and the Supplier is interested in providing them, as set forth in and subject to the tender documents and this Agreement.

It has therefore been agreed, declared and stipulated between the parties as follows:

0. Definitions, interpretation and contradiction between documents

0.1. In this Agreement, the definitions as made in the tender documents are to be used for interpretation unless otherwise stated.

0.2. The Agreement exhausts the covenants between the parties and no negotiations and/or understanding and/or consent and/or representation, whether written or in writing, explicit or implicit, between the parties in relation to the engagement that is the object of the Agreement prior to its execution will have any effect.

1. introduction

1.1. The introduction to this Agreement, including all declarations included and the appendices to the Agreement, along with the tender documents, constitute an integral part hereof and will be interpreted here with unless otherwise stated.

The appendices to this Agreement are:

Appendix B1 – the Supplier's bid for the tender

Appendix B2 – the consideration

Appendix B3 – performance guarantee printout (digital)

Appendix B4 – insurance requirements

Appendix B5 – information security requirements

Appendix B6 – nondisclosure and no conflicts of interest commitment

Appendix B7 – undertaking of an Israeli representation office for a Supplier whose place of residence is outside of Israel

2. Interpretation and contradiction between documents

2.1. In any case of contradiction or discrepancy between the bid of the Supplier, as approved by the Division, and the Agreement and/or the remaining appendices of the Agreement, in part or in full, the provisions of the Agreement and its appendices will take precedence over the bid of the Supplier, **Appendix B1**, and the default is that the provisions most benefiting the Division will apply.

2.2. In this regard it should be improved that in the case of the scope of work set forth in the Suppliers bid is greater or broader than that required in the agreement documents, the Suppliers will provide its services as set forth in its bid and will also fulfill all of the other conditions appearing in the Agreement and in its other appendices.

2.3. The tender documents and any instruction that the Division has given in writing after publishing the tender and before the deadline for submitting the bids, by way of an amendment or modification to the tender and/or giving a clarification to the tender bidders will be considered as an integral part of the Agreement documents. A later instruction will take precedence over any instruction contradicting it in the previous documents, unless otherwise stated in the late amendment and/or clarification.

2.4. In the case of contradiction between the content of the appendices and the content of this Agreement, the provisions of this Agreement will take precedence, and the appendices will be interpreted accordingly.

2.5. If the Supplier has discovered a contradiction and/or discrepancy and/or ambiguity and/or obscurity in its opinion between one of the provisions of the Agreement and another provision of the Agreement, or the Supplier had doubts as to the correct interpretation of the provision, document or any part thereof, the Supplier is to contact the Division before signing the Agreement or immediately after discovering the same, and the Division will provide clarifications and/or instructions in writing on the interpretation that is to be followed. The decree of the Division in relation to a contradiction and/or discrepancy and/or obscurity as set forth above is final, is subject to the sole discretion of the Division and binds the Suppliers to all intents and purposes.

3. Declarations and undertakings of the Supplier

3.1. The Supplier and its delegates hereby declare and warrant towards the Division as follows:

3.1.1. That it has a suitable professional background, know-how and skill that allow it to perform the service according to the tender, the bid and the other provisions of this Agreement, and that it possesses the tools, know-how, means and qualifications to fulfill exactly and fully the requirements of the Division in this

Agreement and all appendices hereto.

3.1.2. That it is a corporation duly registered and operating according to the statutes of the State of Israel or its place of residence, and that no action whose purpose or possible consequence is its liquidation, winding up of its business affairs, a settlement with its creditors, including a going concern remark in its financial statements, striking it down or any other similar consequence, has been taken against it and to the best of its knowledge is not expected to be taken against it.

3.1.3. To the extent that it is a supplier whose place of residence is outside of Israel, that it is aware that it is required to engage with an Israeli representation office, or it has a representative in Israel and will have it sign an appropriate declaration attached as Appendix B7 hereto. If the Supplier replaces a representation office, it undertakes to inform the Division in writing 90 days in advance of the details of the new representation office.

3.1.4. That there is no prohibition, restriction or impediment, including statutory, contractual or pursuant to the foundation documents of the Supplier, to engage with the Division in this Agreement and perform its undertakings hereby.

3.1.5. That the signing of the Agreement by the authorized signatory and executing undertakings pursuant to it have been duly approved by the competent organs of the Supplier, and that the execution of its undertakings thereby constitutes no breach of its incorporation documents or those of any delegate thereof or any other document or promise or undertaking to which the Supplier is a party or of any ither statute or contract or undertaking.

3.1.6. That it is signing this Agreement after having carefully examined and understood the tender and has received from the representatives of the Division all of the explanations and directions it needs and that have been required by it to form its bid and undertakings according to it and according to this Agreement, and that it will have no argument towards the Division in relation to insufficient disclosure or nondisclosure, any error or defect in relation to the figures or facts related to the provision of the services hereunder.

3.1.7. That it undertakes to act in all matters relating to performing this Agreement with the highest expertise and professionalism. The Supplier warrants that the tools, know-how, means and qualifications set forth above will continue to be in its possession until the full discharge of all of its obligations hereunder.

3.1.8. That throughout the engagement period, the Supplier will fulfill the threshold conditions defined in the tender.

3.1.9. That to the extent that additional parties and/or subcontractors have been presented by it within its bid for the tender, the Supplier will sign with these parties a binding agreement according to the requirements hereof, throughout the engagement period, whereby they will provide the Supplier all of the relevant services on which the Supplier has relied for submitting its bid.

3.1.10. That throughout the Engagement and Option Period, it will possess all confirmations and licenses required according to this tender and according to any

statute, in effect, and will present them to the Division immediately upon their renewal from time to time.

3.1.11. That it undertakes to fulfill the Agreement in good faith and faithfully and to do everything required of an expert that is acting for performing the services hereunder.

3.1.12.

3.1.13. That all of the representations and undertakings of any delegate thereof according to the tender documents and the Agreement will remain in effect from the time of submitting the bids for the tender and throughout the engagement and options period; and that it will notify the Division immediately in the case of any change in a representation or undertaking that has been given within the Agreement by it, which may affect its ability to perform the services. the Supplier represents and agrees that its notice pursuant to this section does not constitute the consent of the Division to any change and does not derogate from any right or argument that the Division has according to the contract or any statute;

Section 3 above including all subsections thereof is part of the highlights of the Agreement and its breach will be considered a fundamental breach hereof.

4. The Services essence and undertakings of the Supplier

4.1. The Supplier undertakes to provide all of the Services specified in the tender documents.

4.2. The Services will be provided efficiently and professionally, with attention to the schedules and according to the order of task prioritization as determined by the Division.

4.3. The Services will be provided to the Division and to the governmental medical centers. It should be clarified that the engagement is between the Supplier and the Division only and that the Division will also manage the services for the medical centers, according to all provisions hereof.

4.4. Without derogating from the foregoing, the Supplier undertakes as follows:

4.4.1. To provide all of the required Services, including logistic and professional services, as defined in the tender documents, in this Agreement, and in the Suppliers bid, to the satisfaction of the Division.

4.4.2. To employ professional, experienced personnel that is required and appropriate for the performance of the services, as prescribed in the tender documents, in the suppliers bid, of the best professional quality.

4.4.3. To provide the services faithfully, with expertise and the best professionalism and bear the exclusive responsibility for the nature, quality and results of the service.

4.4.4. To make adjustments, modifications and improvements in the future according to the requirements of the Division, in accordance with the provisions of this

Agreement and the tender documents.

4.4.5. To meet the schedule required according to the provisions of the Agreement and the tender documents and to make available to the Division all means required for performing the services at the availability level, to the volume and under the conditions mandated by the prescribed schedules.

4.5. To provide regular reporting and answer any request, whether in writing or oral, to the Division and its representatives on any matter related to the performance of the services and the deliverables that will be submitted within this Agreement on any matter that will be required.

4.6. The Supplier is aware that the Division has many suppliers operating for it, some of which may be its competitors, and it undertakes to cooperate with them for the provision of the services that are the object hereof and for the parties to accomplish their objective. The Supplier hereby gives its consent to the effect that any information on the services that have been provided by it will be forwarded to another supplier to get a professional opinion, at the discretion of the Division. If the supplier causes costs / delays of a third party towards the Division, it undertakes to indemnify and/or compensate the Division.

4.7. The Division will be able to demand that the Supplier perform changes to the required services, according to Regulation 3C of the Mandatory Tenders Law Regulations 5753-1993. Any change to the conditions of the Agreement and/or its appendices will be made with the advance written consent of both parties, subject to approval by the automatic data processing tenders committee of the Division. Waiver by way of conduct will not be considered as a waiver of a right arising from this Agreement.

4.8. The Supplier will not have exclusivity in receiving works from the Division and the Division will be able to receive the services of the type that are the object hereof and of any other type from any other party. The Division will reserve the right not to demand from the Supplier or from any other party any services, and perform these services by itself, at the Divisions sole discretion.

This section is a fundamental condition of the Agreement.

5. The engagement period

5.1. The engagement period within this tender is starting from the date of signing of this agreement by the parties **for 10 (ten) years** (hereinafter: the "**Engagement Period**".

5.2. Right of choice

According to the provisions of Regulations 3C(A) of the regulations and subject to getting approval from the automatic data processing tenders committee, the Division will reserve a right of choice both in relation to the duration of the engagement period and its scope, as follows:

5.2.1. The Division will be allowed to extend the engagement period by 2 additional periods lasting up to 5 years each, whose total duration will not exceed 10 years

cumulatively (hereinafter: the "**Option Period**").

5.2.2. The Division reserves the right to exercise one or more Option Periods at any time of exercising a right of choice.

5.2.3. The Option Period will be exercised subject to the decision of the tenders committee, which will be brought before the committee at least 60 days before the end of the Engagement Period. The Supplier must announce 90 days before the end of the relevant Engagement Period.

5.2.4. The total Engagement Period with the Supplier, in addition to the Option Periods, will not exceed 20 years in total, subject to the needs of the Division and budget restrictions.

5.2.5. Throughout the Option Periods, all conditions of the Agreement will apply to the Supplier, mutatis mutandis, including the duty to provide a current performance guarantee and provide a current confirmation of execution of insurances.

5.2.6. If services are ordered from the Supplier before the end of the Engagement Period or the Option Period (as relevant) and the Supplier does not complete the services by the end of these periods, the relevant period will be extended until the said services are finished. It should be clarified that in any case additional services will not be ordered after the end of the Engagement Period / Option Period (as relevant).

This section is a fundamental section hereof.

6. Representatives

6.1. The representative of the Division for the purpose of executing this Agreement is the project manager in the Information Systems and Work Processes Division, while a notice of the identity and contact details thereof will be forwarded to the Supplier at the time of implementing the engagement (hereinafter: the "**Division Representative**").

6.2. The Division is allowed to replace its representative and/or representatives at any time by giving the Supplier written notice.

6.3. The Supplier undertakes to follow the instructions of the Division Representative relating to implementation of the tender requirements.

6.4. On all matters relating to executing its professional services, the Supplier will be in contact with the Division Representative, which will also oversee the works of the Supplier. The Division Representative will be allowed from time to time to demand that the Supplier perform additional tasks that are included in the broad range of the requirements of the tender and the qualifications of the service provider.

6.5. The Suppliers representative (hereinafter: the "Managerial Representative") for the purposes hereof is Name: _____ Address _____ Email: _____ Mobile: _____.

6.6. In the case of substitution of the Managerial Representative, the Supplier undertakes to notify the Division ~~30~~ 60 workdays before the expected date on which he is to

conclude his function and get its written approval. In any case, the outgoing Managerial Representative will finish his function only after the approved substitute representative enters. Without derogating from the statements in the sections above, the Division will be allowed at any time to demand that the Supplier substitute its Managerial Representative and any other members of the team providing the services to the Client, without any compensation, indicating the reason for the replacement. It should be clarified that the Division is not required to state the reason for the substitution and the Supplier undertakes to do so within 30 workdays. In the case of immediate substitution of the representative, the Supplier will provide the Division a substitute representative until the position of the Managerial Representative is manner within 30 workdays as set forth.

6.7. The Supplier will report to the Division Representative through the Managerial Representative about the service that is being provided on a monthly basis and according to the service form (reporting of hours, outputs, etc.).

7. Responsibility

7.1. The Supplier will be responsible for the manner of provision and quality of the services, the responsibility is inter alia for full, comprehensive performance of the Services.

7.2. In the case of a license or certificate required within this tender and that has expired, the Supplier is responsible for making sure that they are renewed and immediately announcing this to the Division.

This section is a fundamental condition of the Agreement

8. Third party products warranty period

8.1. Any purchase of a third-party product that will be supplied by the Supplier, even if no longer installed at the Division, will include a warranty of one year from the time of confirmation of the completion of the installation by the Division.

8.2. Throughout the engagement period, the Supplier will also be responsible for the manner of provision and quality of the services. The warranty is inter alia for full, comprehensive performance of the services.

8.3. The warranty of the Supplier will apply in full to all elements of the System including repairing any malfunction in third party elements of the System that have been provided by the Supplier.

8.4. In the case of a license or certificate required within this tender that has expired, the Supplier is responsible for ensuring that it is renewed and announcing this to the Division immediately.

9. Non-exclusivity

9.1. The Supplier will have no exclusivity in the provision of the Services and the Division will be able to receive the Services of the type that is the object of this Agreement and of any other type from any other party.

9.2. The Division will reserve the right not to ask the Supplier or any other party for any Services, and perform these Services by itself, at the Division's sole discretion.

10. Control and supervision

10.1. The Division will conduct, at its sole discretion, or will demand that the Supplier conduct, random checks to tests the Services that will be provided to the Division, whether by the Supplier itself or by any of the Supplier's subcontractors.

10.2. The Supplier undertakes to cooperate with the Division Representatives in relation to performing the Services and fulfilling all of its other obligations according to the Tender and the Agreement, and will fulfill any direction of the Division Representatives, subject to the provisions of the tender and the Agreement. As part of this, it will provide any information or report that will be required by them, at the time or in the manner that will be determined thereby.

11. Ownership and copyrights

11.1. It is agreed by the parties that the basic platform as an "off the shelf product" will be owned by the Supplier. The Client will be provided a right of use, without any additional or other license conditions applying to the Division besides those explicitly stated herein. If the proposed solution includes third party usage rights, the Supplier will make sure to arrange these rights for the Division, without having to have the Division sign an agreement or any agreement besides the agreement between it and the bidder and without the need to charge any additional cost.

11.2. It is agreed by the parties that any future development (development and/or adjustment that will be performed on an off the shelf product) that has been performed upon the demand of the Division and developed for its needs, as a separate, distinct module, will be owned by the Division, including all deliverables thereof (appendices, drafts, charts, plans, etc.), and the Supplier and/or its delegates will have no right thereto and will not be allowed to transfer it or disclose any detail thereof to a third party except with the advance written permission of the Division.

11.3.

11.4. For the removal of doubt, it is hereby clarified that all information, data, documentation and reports that will be stored in the System or produced using it, within its use by users on the part of the Division, are the exclusive property of the Division and the Supplier will have no right to make any use thereof.

11.5. The Supplier declares that it has not infringed and will not infringed on any copyright

and/or patent and/or commercial secret during the performance of its commitments hereunder.

11.6. In any case of a third party claim on account of the services infringing on a copyright and/or patent and/or commercial secret or open source license, the statements in Section 21 below will apply.

12. Performance guarantee

12.1. For securing the obligations of the Supplier in a professional, high-quality manner within this Agreement, and as a condition to signing it, the Supplier or its representative (in the case of residing outside of Israel) will provide to the order of the Division, within fourteen (14) business days from the time of receiving a notice, an unlimited autonomous guarantee under conditions to a volume that will be calculated based on 5% of the Division's estimate of the volume of the Annual Services (hereinafter: "**Performance Guarantee**"). The Di~~i~~vision is allowed to update the among of the guarantee each year according to the expected scope of the engagement that year.

12.2. It is clarified that the provision of the said guarantee constitutes a precondition to the provision of the services to the Division. If the Supplier has not deposited a guarantee as required by the time prescribed by the Division and/or has not fulfilled any other condition in these requirements, this will be considered as failure to fulfill its obligations pursuant to this Tender and it will have no argument on failure to implement the engagement, with all resulting consequences.

12.3. The Performance Guarantee will ~~not~~ be linked once a year to the Israeli consumer price index~~.~~

12.4. **Israeli supplier** – the guarantee will be a digital guarantee and will be drafted and managed as stated in the provisions of Takam [regulations, articles and housekeeping] 14.4.1

12.5. The digital guarantee will be produced by one of the entities in the list of entities authorized to issue a digital guarantee pursuant to this instruction. An example of a digital guarantee text is attached to this Agreement as Appendix 3B hereto.

12.6. **Overseas supplier** – the Supplier will be able to choose and provide a digital guarantee as set forth in Section 12.1.1 above. If not possible, after getting advance permission from the Division, it may submit a manual guarantee, that will be made according to Section 2.2 and the provisions of Takam 7.3.3.1.

12.7. The Performance Guarantee will be in effect throughout the Engagement Period plus 60 days after its conclusion.

12.8. If the Division decides to exercise the Option Periods available to it within this Agreement, the guarantee will be extended accordingly and the Supplier undertakes, to secure its obligations according to the extended agreement, to provide the Division no less than 14 days before the start of the Option Period a valid guarantee. This guarantee will be in effect up to 60 days after the end of the extended service provision period.

12.9. In any case of the Supplier not meeting its obligations according to the Agreement and/or by statute and/or subjecting the commencement or continuation of the provision of service to financial and/or other demands and in the case of the Division having lawfully exercised its rights and paid amounts applicable to the ~~sums payable by the~~ Supplier according to the Agreement or any statute, the Division will be entitled to invoke some or all of the guarantee, subject to giving the Supplier 14 days' advance written notice to give an opportunity to rectify the nonfulfillment of the obligations, in cases in which the breach was not rectified by the Supplier.

12.10. If the Supplier did not meet its said obligations, the invocation of the Performance Guarantee will be deemed as liquidated damages as defined in Section 15 of the Contracts Law (Remedies for Breach of Contract) 5731-1970 to the benefit of the Division. The statements in this section do not derogate from the right of the Division to any other relief pursuant to this Agreement or any statute for the breach.

12.11. For the removal of doubt, it is clarified that the guarantee amount does not serve as a restriction or limit to the undertakings or warranty of the Supplier hereunder.

12.12. If the guarantee has not been invoked, the guarantee will be returned to the Supplier within 60 days of the Engagement Period ending and the Division confirming that the services have been provided to its full satisfaction.

13. The consideration

13.1. Consideration for performing the services will be determined according to the winning supplier's bid, Appendix B7.

13.2. 0The consideration is fixed, absolute and final and the Supplier will not be allowed to demand increases or changes from the Division for performing its duties hereunder, for any reason.

13.3. It should be clarified that this Agreement does not bind the Division to pay any consideration, and the only undertaking will be according and subject to approved work orders as issued by the Division from time to time, subject to actual performance.

13.4. No payments will be made for expenses that have not been defined in the work order, including office expenses, travel and payment of wages, preparation and organization expenses for performing the services, including any other direct or indirect expense, arising from provision of the services and including the profit of the Supplier. For the removal of doubt, the Supplier has considered in the bid all costs stated above and has grossed them up within it.

This section is a fundamental condition to the Agreement

14. Linkage

14.1. All prices will be stated in U.S. dollars without VAT.

14.2. A supplier that is not registered in Israel will receive payment in dollars according to

the representative exchange rate on the deadline for submitting bids for the tender.

14.3. An Israeli supplier will receive payment in NIS including statutory VAT and linkage to the dollar exchange rate. The linkage will be calculated according to the base rate on the deadline for submitting bids for the tender.

15. Payment method

15.1. The Supplier will submit an invoice along with a written confirmation from the Representative of the Division for eligibility for payment, as set forth in Appendix B2 to the Agreement.

15.2. For the removal of doubt, it is hereby clarified that the confirmation of a bill, in part or in full, and/or making the payment for it, in part or in full, will not constitute evidence of the correctness of the statements therein and/or the nature of the services that were performed by the Supplier or derogate from the provisions hereof.

15.3. A bill that is found to be improper by the Division, including owing to failure to attach the documents and/or references that the Supplier must attach and/or a bill will not be considered as a bill submitted on time and its submission time will be only the time at which a bill will be resubmitted and found to be proper.

15.4. The Division will check the bill and will be able to demand modifications / adjustments, by explained written notice, within up to 30 days of the day of the bill being submitted and/or the supplementations being provided, as relevant.

15.5. The payment conditions will be according to the Takam instructions 1.4.3 or in accordance with the current Takam instructions as published from time to time.

15.6. The Supplier or a delegate thereof will be required to submit reports and invoices through the governmental suppliers portal, a computer system of the Government that supports inter alia online submission of invoices.

15.7. To this end, the Supplier will sign a suppliers portal usage contract, which is prescribed in Takam instructions 7.12.5 – suppliers portal, and will perform all actions required of it for connecting to the portal, or the supplier will produce a confirmation that it is already using the suppliers portal, as stated in the Takam instruction.

15.8. Subject to legal obligation, each payment that the Division will make to the Supplier pursuant to this Agreement will include VAT, according to the VAT rate in effect at that time. The Supplier undertakes to transfer the VAT payment to the tax authorities according to any statutory provisions and directions of the tax authorities and transfer a tax invoice to the Division.

16. Work relations between the parties

For the removal of doubt, it is agreed between the parties that:

16.1. The relations between the Division and the Supplier, its employees and delegates in performing this agreement are client – supplier relations and there are no employer –

employee relations between the supplier, or any party employed on its behalf, in performing this Agreement, and the Division and/or any delegate thereof.

16.2. The Supplier and all persons employed thereby in performing this Agreement will have no rights of a civil servant or a worker employed by the Division, and they will not be entitled to any payment, compensation or other benefit in relation to performing or finishing this Agreement.

16.3. The actions of the Division or its delegates that are provided pursuant to this Agreement, such as oversight, instructing, directions or instructions to the suppliers or any delegate thereof in relation to the services serve as a means to secure performance of the provisions hereof only and/or achieving the goals hereof in their entirety, and for securing the manner of performance of the services by the Supplier and nothing more.

16.4. The Supplier only will bear the taxes and other mandatory payments that an employer must pay in relation to its employees and according to the statutes and practice at the place of residence of the Supplier and/or in Israel, including payments for national insurance, parallel tax and all other social rights, and the Supplier only will be responsible for any claim that will be filed against the Division and/or against the Supplier by an employee of the Supplier arising from the labor relations between them.

16.5. If notwithstanding the clear intent of the parties as set forth above, if it is pronounced one day by a competent judicial instance that there are employer – employee relations between the Division and the Supplier, with all resulting implications, the Supplier undertakes, without derogating from the statements herein in general, to indemnify the Division immediately for all expenses that it will sustain, including expenses and payments that it will be charged and trial expenses and attorney fees. The provisions of Section 21 below will apply to the indemnification conditions.

16.6. The Supplier or its delegate undertakes to fulfill throughout the period of the Agreement, for the employees who will be employed by it in performing the services hereunder, the provisions of the labor statutes applying in the State of Israel or the statute prescribed in its place of residence.

16.7. The Supplier or its delegate hereby undertakes not to employ, directly or indirectly, a person employed by the Division as long as this Agreement is in effect and for 18 months from the day of the engagement ending, except with the prior written permission of the Division.

16.8. Any engagement of the Supplier with subcontractors for the sake of providing the services is an engagement of the supplier with the subcontractors only and does not form any employer – employee relations between the subcontractors and the Division. However, the Supplier warrants that any service that will be provided to the Division within this Agreement, whether provided to the Division by it or by the subcontractor on its part, will fulfill all of the requirements and conditions set forth in this Agreement and its appendices.

16 Nondisclosure

16.9. For the purposes of this section –

16.9.1. Secret information is as defined in the tender.

16.9.2. The Supplier, its employees and delegates involved in the provision of the services within the Agreement, undertake to keep secret and not transfer, announce, disclose or bring to the attention of any person any information that will reach them during or due to the execution of this Agreement during the agreement period or thereafter.

16.10. The parties mutually undertake to keep secret any secret information that will reach their knowledge during and/or in relation to the execution of this Agreement, including any document, plan, drawing, software, work instructions, performance procedures and/or any other information that has reached its knowledge during the execution hereof and/or in relation with its performance.

16.11. However, for information that the Division will notify the Supplier of as being considered secret information, even if not falling under the definition of secret Information – the Supplier will make every effort to safeguard it in accordance with the provisions hereof.

16.12. The Supplier declares that it is aware that taking information out of the premises of the Division or using information that has reached it within the provision of the services other than for the direct purpose of providing the Services is strictly forbidden.

16.13. For the removal of doubt, it should be clarified that the provisions of Sections 117 and 118 of the **Penal Law, 5737**-1977 will apply to a breach of the duty of secrecy and a breach of the duty of secrecy will constitute a fundamental breach hereof.

16.14. An undertaking according to this section will survive the end of the Engagement Period.

16.15. The Supplier undertakes to notify its employees and persons employed by it and/or on its behalf in relation to this Agreement of the commitment to secrecy set forth below.

16.16. As a condition to starting the provision of the services by the employees and/or delegates of the Supplier, they must sign a full nondisclosure agreement, before starting their activity, in the form of **Appendix B6** to the Agreement, whereby they are aware that the non-fulfillment of an obligation according to this section constitutes a violation of Chapter F, Article E of the Penal Law, 5737-1977. It should be clarified that the foregoing does not derogate from the undertaking of the Supplier to safeguard secrecy as required herein.

This section is a fundamental condition to the Agreement

17 Prevention of conflicts of interest

For the purposes of this section:

"Stakeholder" – as defined in the **Securities Law, 5728-1968.**

"Employee" – any of the employees of the winning Supplier, including and party on its behalf.

The "**Supplier**" – including, in addition to the Supplier itself, its employees and service providers, and for all of them, including their partners, relatives, directors and stakeholders therein.

"**Relative**" – a spouse, sibling, parent, issue and any parent or spouse of any of the foregoing.

"**Conflicts of interest**" – the occurrence or genuine, substantiated fear of occurrence, in the opinion of the Division, of the Supplier being in any of the following states:

A. A clash between the duty imposed on the Supplier to perform its function according to the Agreement without foreign considerations or impartially, and any other interest of the Supplier (as this term is defined below).

B. Being in a "**personal conflict of interest**", i.e.: when any interest entrusted to the Supplier hereunder may clash with any other interest thereof.

C. Being in a "**moral conflict of interest**", i.e.: when any interest entrusted to the Supplier hereunder may clash with any other function, public or private, which it has within a public body or other entity.

17.1 The Supplier declares that to the best of its knowledge, after a thorough check:

17.1.1 It has and does not know of any conflicts of interest in performing its commitments under the Agreement.

17.1.2 It has and does not know of any other conflicting interest.

17.1.3 Subject to the statements in this section, the Supplier will not be in a state of conflicts of interest throughout the period of the Agreement and for a year after the period of the Agreement.

17.1.4 The Supplier declares that on any matter in which concern arises of a state of conflicts of interest in the service provided by it hereunder, even if it is unsure of this, the Supplier will contact the Division and will follow the Division's directions. If the requested action has no true relation to the service provided hereunder or there are other circumstances, the Division will provide guidance accordingly.

17.2 In any case in which concern arises of conflicts of interest or the occurrence of any conflicting interest:

17.2.1 The Supplier will notify the Division within 3 business days of any event or circumstance that may lead to a state of conflicts of interest and any conflicting interest. The Supplier will follow the instructions that the Division will give it as set forth below.

17.2.2 The Division is allowed to demand from the Supplier any information as it sees fit in order to find out the facts and circumstances relating to the occurrence of concern of conflicts of interest, which information will be provided without delay.

17.2.3 The Division is allowed, at its sole discretion, to subject the intent of the Supplier to engage with any party to instructions, if the engagement may cause a conflict of interest, and the Supplier will follow these instructions.

17.2.4 If the Supplier has refused to follow the instructions of the Division or has acted in a manner that does not satisfy the Division, the Division is allowed to order the termination of the engagement with the Supplier and ending of the engagement therewith for this reason only and the starting of the activation of the separation plan as set forth in the tender documents. The termination of the engagement with the Supplier will occur after it has been given an opportunity to assert its arguments in writing, within the time prescribed by the Division.

17.3 The foregoing does not derogate from the right of the Division to act as set forth, whether if the Division learns of the concern due to the information that the Supplier has provided it or in any other way.

17.4 Notwithstanding any provision to the contrary in this section, the Division will be allowed to permit the Supplier to continue to provide the services according to the Agreement even if there a conflict of interest has occurred as long as it has examined the aspects and deemed it possible to continue the engagement despite an occurrence of conflict of interest.

17.5 The Supplier and all parties on its behalf directly involved in the provision of the Services to the Division will be required to sign without any reservation a nondisclosure and no conflicts of interest agreement appendix, in the form attached hereto as Appendix B6.

17.6 Without derogating from the other provisions of the Agreement, as a condition to this Agreement taking effect will be providing the above-mentioned Appendix and confirmation of the legal office of the Division, if the Supplier has declared a conflict of interest and/or concern for conflict of interest in relation to the requested services, as of the time of giving the declaration.

This section is a fundamental condition to the Agreement

18 Publication

It is hereby agreed that any publication on anything related to performance and/or provision of the Services will be done in coordination and with mutual consent between the parties and after getting permission from the Ministry of Health's spokesperson unit in Israel.

19 Tortious liability

19.1 The Supplier will bear liability for any damage inflicted on the Division and/or the Ministry or on any third party due to a professional act or default, error or omission committed intentionally or recklessly or negligently by the Supplier and/or any employee and/or proxy

and/or subcontractor thereof within their actions hereunder.

19.2 Limit of liability –

19.2.1 The limit of the Supplier's liability for compensation or indemnification for any damage event for which the Supplier is responsible according to the provisions hereof will not exceed the amount of the damage inflicted or the indemnification sum that is required and up to **2 times the volume of the total consideration of this Agreement hereunder**, plus all of the Division's expenses, including legal expenses and attorney fees that it will incur in relation to a claim for the foregoing, and any addition of linkage differentials and statutory interest.

19.2.2 The limit of liability will not apply to damage in the following cases:

19.2.2.1 Damage that has been inflicted intentionally or dishonestly through an act or omission of the Supplier, its employees or delegates.

19.2.2.2 Damage that has been inflicted on a third party by an act or omission of the Supplier, its employees or delegates.

19.2.2.3 Damage that is covered by insurances that the Supplier has undertaken to execute hereunder.

19.2.2.4 Damage to tangible property or damage that is bodily harm, death, disease, injury, physical, mental or cognitive disability.

19.2.2.5 Damage that has been inflicted as a result of a breach of the duty of secrecy.

19.3 The Supplier undertakes to indemnify the Division fully for any expense that it incurs owing to a charge that the Supplier owes according to this Agreement or any statute, including attorney fees and trial expenses. Provisions on the matter of invoking the indemnification are set forth in Section 21 below.

19.4 It is agreed between the parties that the Division is not responsible for and will not bear any payment, expense or damage for any reason that will be sustained by the person or property of the Supplier or any delegate thereof, or the person or property of its employees or any delegate thereof, or by the person or property of any other individual as a direct or indirect results of performance of this Agreement and that this responsibility will be borne by the Supplier only, unless the damage was inflicted owing to gross negligence or malice on the part of the Division.

This section is a fundamental condition to the Agreement.

20 Legal proceedings in the case of indemnification that is required of the Supplier

20.1 To the extent that the Supplier assumes a duty of indemnification, the provisions of this section below will apply.

20.2 The Division will inform the Supplier of a contact, demand or claim that has been filed before it on a matter related to this Agreement, shortly after the demand or claim arrives; alternatively, if the Supplier receives a contact, demand or claim in the context hereof, it will inform the Division shortly after receiving them.

20.3 If the Supplier is a party to the claim, the Supplier will manage and finance its defense, whether in a legal proceeding or in a settlement proceeding in advance arrangement with it and after receiving the consents of the Division on the manner of managing the legal proceeding and/or settlement proceeding, without the Supplier being allowed to admit anything on behalf of the Division;

20.4 If the Division is a defendant in the proceeding – it will manage the defense by itself at is sole discretion, including choosing experts and legal representation, etc. The Division will be able, at its discretion, to issue a third party notice to the Supplier.

20.5 If the Division asks to settle, it will update the Supplier accordingly.

20.6 The indemnification from the Supplier to the Division will be made when the Division is required at any time to make any expense, including but not limited to expenses incident to the legal proceeding (attorney fees, court fees, expert fees, etc.) will be according to and subject to a final judgment of a competent court.

21 Information security

21.1 Without derogating from its obligations pursuant to the sections of the tender and/or the information security appendix attached as **Appendix B5**, the Supplier undertakes as follows:

21.2 To be responsible towards the Division for any information that has been forwarded to the possession of the Supplier within this Contract, including on: Reports, forms, magnetic media or information about personal data, information systems and the registry of healthcare institutions in particular and the Division in particular.

21.3 To see to securing of all information and material that has reached it within the execution of its duties hereunder and show the information security means to the representative of the Division upon its demand.

21.4 To prevent access to the computer systems of the Supplier or serving it for the purpose of executing the services pursuant to this Contract from a person that is not a partner in the provision of the services or a party that is not authorized to view the material or information stored in a computer or a party that has not signed the nondisclosure agreement attached as **Appendix 6B** hereto.

21.5 To ensure that all its employees and subcontractors will safeguard the information as set forth in the Protection of Privacy Law 5741-1981.

22 Insurance

22.1 The Supplier undertakes to purchase and maintain all of the insurances set forth in Appendix **B4**, the insurance requirements appendix (hereinafter: the "**Insurance Appendix**") to its own benefit and that of the State of Israel- the Ministry of Health, including the coverages and conditions required, the limits of liability being not less than those stated in the Insurance Appendix attached hereto.

22.2 The Supplier undertakes to forward the insurance confirmation as set forth in the Insurance Appendix that will be shown by the Supplier from its insurers, presented in a uniform format according to the directions of the Control of Insurance that will be in effect at the time of issuing the confirmation, containing the details whose details may be shown, according to the demand of the Division.

22.3 It should be clarified that the Division will forward its demand to receive an insurance confirmation within 14 days of the time of the notice to the Supplier of winning the tender.

23 Professional liability insurance

23.1 The Supplier will cover its professional liability by professional liability insurance.

23.2 The policy will cover damage from breach of a professional duty by the Supplier, its employees and for all delegates acting on its behalf that has occurred as a result of an act, negligence, including a default, error or omission, misrepresentation, negligent declaration made in bad faith, which will be sustained on any matter related to provision of the services for providing a platform for the development and implementation of planning, budgeting and organizational performance management solutions, its installation and maintenance, for the Governmental Medical Centers Division, the Ministry of Health, according to the tender and a contract with the State of Israel, the Governmental Medical Centers Division, the Ministry of Health.

23.3 The limit of liability will not be less than 250,000 U.S. dollars per case and for the insurance period (a year).

23.4 The coverage according to the policy will be expanded to include the following expansions:

A. Employee fraud and dishonesty;
B. Loss of documents, including loss of use and/or delay due to an insurance case;
C. Cross liability, but the coverage will not apply to the cases of the Supplier against the State of Israel – the Governmental Medical Centers Division, the Ministry of Health;
D. Extension of the disclosure period for at least 6 months.

23.5 The insurance will be expanded to indemnify the State of Israel – the Governmental Medical Centers Division, the Ministry of Health, to the extent that they are considered responsible for acts and/or omissions of the Supplier or its delegates.

24 Right of offset and lien

24.1 The Division is allowed to offset or withhold any sum that is owed to it from the Supplier, including but not limited to a sum owed to it for damages according to this Agreement and as a result hereof, or from provision of partial services or overpayment.

24.2 The offset and/or lien (as relevant) will be made from any sum that is owed to the Supplier by the Division through offsetting from the last payment and/or the upcoming payment and if there is no future payment, the sum will be deducted from the Performance Guarantee and/or in any other way at its sole discretion, after giving the Supplier 14 days' advance notice before making the offset.

24.3 In any case, the Supplier will have no right of lien or offset against the Division.

25 Prohibition of assignment of rights and duties

25.1 The Supplier will not forward to another party its rights and duties hereunder, including any right and/or duty arising from it, unless it has received prior written permission from the Division to do so including assignment and/or transfer inside the Supplier's group (to subsidiaries / sub-subsidiaries / related companies) as long as the Supplier reports to the Division and gets its approval to do so and forwards a corresponding undertaking for its responsibility and the responsibility of the transferee towards the Division.

25.2 For the removal of doubt, it is hereby clarified that in any case in which an assignment of rights and/or duties as set forth above is made, it does not exempt the Supplier from responsibility towards the Division hereunder.

25.3 The Division is authorized to assign its rights to the services and/or the solution to any other governmental public entity, according to its decision and prior notice, without changing the duties and rights of the Supplier hereunder.

26 Termination or reduction of the engagement –

26.1 The Division reserves the right to terminate the engagement and/or reduce its scope at any time and for any reason, before the Engagement Period has ended and during the Option Periods, without assuming any duty to give reasons for doing so.

26.2 The termination of the engagement and/or reduction of its scope will be done subject to giving 120 days' advance written notice (hereinafter: the "**Advance Notice**").

26.3 In any case of termination and/or reduction of the engagement as above, the Supplier will have no arguments and/or claims and/or demands for payment and/or compensation in relation to the said actions of the Division after the time of sending the Advance Notice, except for payment for services that have been provided before the end of the engagement, and a refund of expenses for orders that were made with the advance written approval of the Division that cannot be cancelled. Actions that involve any additional costs, which the

Supplier has taken after the time of sending the Advance Notice, without receiving an explicit instruction from the Division, will not be paid for.

27 Breach of the Agreement and remedies owing to its breach or cancellation

27.1 The Division will be allowed to terminate the engagement with the Supplier after sending 14 days' advance written notice in any of the following cases (this period will be considered as a period for recertification of the breach by the Supplier).

27.2 In the case of the Supplier having committed a fundamental breach of the Agreement as set forth herein.

27.3 In the case of the Supplier not fulfilling one or more of the tender's threshold conditions or representations made within the answer to the tender (including in relation to the solution's capabilities).

27.4 In the case of the Supplier having violated the information security instructions.

27.5 In the case of the Supplier ceasing to serve as an official representative of the solution's manufacturer (if relevant).

27.6 In the case of a motion for instigating an insolvency proceeding is opened on the part of the Supplier or any of its creditors under the Insolvency and Economic Rehabilitation Law, 5778-2018.

27.7 In the case of a temporary or permanent liquidator being appointed for the Supplier.

27.8 If the Supplier has endorsed the agreement, in part or in full, to another party without notification and without the Division's approval.

27.9 In the case of the Supplier having provided services or performed services other than in accordance with the provisions of the Agreement including its appendices and the tender documents.

27.10 In the case of an indictment being filed against the Supplier and/or any of its directors, the Supplier must immediately report this to the Division, which has the sole discretion on whether to terminate the engagement. If it fails to make such a report, the engagement will be terminated immediately upon the Division learning of the indictment being filed, and in any case, the engagement will be terminated pursuant to this section in the case of the Supplier and/or any of its directors being convicted of a criminal offense.

27.11 Violations on the part of the Supplier whose cumulative value in 3 consecutive months exceeds 75% of the relative monthly consideration to the Supplier will constitute a cause for immediate cancellation of the Agreement, at the Division's sole discretion.

27.12 Without prejudice to the entirety of the statements in Section 28.1 above, in certain cases, an amendment notice will be given to the Supplier allowing for a period for rectification of the breach lasting up to 14 days from the time of notice of termination of the engagement.

27.13 In cases of a fundamental breach or a breach as set forth above that cannot be rectified, the Division may order the termination of the engagement even without a rectification notice

to the Supplier.

27.14 A default in or failure to fulfill any of the provisions of this Agreement will not be considered as a breach hereof under the following cumulative conditions:

27.15 The event is not due to the fault of the Supplier (including in the case of force majeure).

27.16 The event directly causes the Supplier to be unable to meet its obligation under the Agreement that leads to its breach.

27.17 The Supplier notifies the Division immediately of the occurrence of the case.

27.18 The Supplier will take any reasonable step to avoid non-fulfillment of the provisions of the Agreement for preventing and/or reducing damage.

27.2.

27.19 If the Supplier does not rectify the breach within the time specified in the notice, the Division will be allowed to cancel the Agreement at the end of the said time and invoke the Performance Guarantee.

27.20 The statements in this section do not derogate from the right of the Division to any other relief pursuant to this Agreement or any statute for the breach.

27.21 It is clarified and agreed by the parties that in the case of the Supplier committing a breach as set forth, it must refund to the Division all payments that have been made to it from the time of the breach.

28 General provisions in the case of termination of the Agreement

28.1 If it is decided to terminate the engagement with the Supplier for any reason, whether due to the conclusion of the Agreement on time or owing to its termination before the end of the Engagement Period, the Supplier undertakes to conclude the provision of the services to which it is committed for orders that applied in the Engagement Period, unless the Division Representative orders otherwise.

28.2 In addition, the Supplier undertakes, upon the demand of the Division, to:

28.2.1 Complete all of the orders made that the Supplier has not yet completed; and

28.2.2 Conduct an orderly handover to and instructing for any other party as the Division will order it, by the time of the termination of the engagement between the Division and the Supplier.

28.3 The Supplier undertakes to act and take all means available to it to reduce and prevent damage as a result of conclusion of the engagement according to this section and cooperate to the extent require in order to allow the Division to continue to receive services properly.

28.4 The manner of transfer of the information at the time of conclusion or termination of the engagement will be as follows:

28.4.1 The Supplier will forward to the Division all document required in accordance with the provisions of **Appendix B1- the required services**, the Division reserves the right to demand to receive the information in parts and

in a number of separate transfers during the information transfer period.

28.4.2 The Supplier will return to the Division all of the files and media files, documents, documentation, clarifications and any other item, on any medium (paper, magnetic or optic media, etc.) pertaining to the provision of the services.

28.5 The Supplier undertakes not to retain any material, information or documentation pertaining to the Division and/or parties related thereto subject to the law, and will document the process of destruction of the data that was in its possession.

28.6 All of the foregoing applies to the Supplier and any of its delegates, if information and data is transferred to subcontractors, the Supplier is responsible for the provisions above to be performed properly by the subcontractors.

28.7 For the removal of doubt, extension and/or termination of the Agreement as stated in this section refers to the entire Agreement or part of it.

29 Clarification of disputes

29.1 The representative of the Division in the clarification of any dispute related to or arising from the provision of the Services hereunder will be under the sole jurisdiction of the Division's automatic data processing tenders committee. It should be emphasized that no other party of the Division has the authority to commit to any change in the content of the Services other than in accordance with the provisions of the tender and this Agreement, and any such undertaking made will be invalid.

29.2 28.2. The existence of inquiries, as stated above, will not in themselves require the cessation of the performance of the services according to this agreement or the cessation of the Division's payments regarding what is not in dispute, both regarding the performance of the Services and regarding the payment.

29.3 The provisions of the Arbitration Law 5728-1968 will not apply to investigations under this section.

30 Sending of notices

All notices pursuant to this Agreement will be sent by registered mail and upon thus being sent will be considered as having reached their destination within 120 hours of duly being sent, unless it has been proved that they have not reached their destination.

30.1 A notice that has been sent by email will be considered as having reached its destination on the first workday after sending – a receipt notice must be sent by reply email and its confirmation confirmed by telephone call.

30.2 The addresses of the parties for giving notices on the matter of this Agreement:

The Division – the Governmental Medical Centers Division, the Ministry of Health, 15 Hatzvi Street, Jerusalem.

The Supplier – as set forth in the title hereof.

30.3 In any case of a change in ownership or address, the Supplier must announce this in writing

without delay to the party responsible.

31 Jurisdiction

The exclusive jurisdiction to hear any action whose cause lies in this agreement will be conferred to the competent court in Jerusalem only.

32 Miscellaneous

32.1 This Agreement exhausts all of the covenants between the parties and upon its signing, no negotiations, declaration, representation, undertaking and/or consent, memorandum, draft agreement, etc., which existed, if any, in writing or rally, explicit or implicit, between the parties prior to signing this Agreement will be in effect.

32.2 The Supplier declares that as of the time of engaging in this Agreement, it is not aware of any statutory impediment that may interfere with the performance of the services hereunder and it is not bound to and/or involved in, directly or indirectly, any matter that may pose concern for conflicts of interest in relation to its obligations hereunder.

32.3 The Supplier undertakes to follow the provisions of any statute and any competent authority in relation to the services and/or execution of the Agreement and everything arising from or involving them.

IN WITNESS WHEREOF the parties have signed

The Governmental Medical Centers Division The Ministry of Health	The Supplier

Attorney confirmation for the Supplier's undertaking above

I hereby confirm that the declaration above was duly signed by the authorized signatories of the Supplier and that no change was made in the wording of the Agreement, as published by the Governmental Medical Centers Division, the Ministry of Health, except in the places marked for completion by the Supplier.

Date	Full name of attorney + LN	Signature and stamp

Appendix B1 to the Agreement: The Supplier's Bid

(will be added after the announcement of the tender winner)

Appendix B2 – the Consideration (from the Suppiler's bid)

(will be added after the announcement of the tender winner)

Appendix B3 – Digital Guarantee Printout

This document is a printout of a digital guarantee and is intended for illustration purposes only

This printout was produced by the system of _____ (name of the issuer of the guarantee / recipient of the guarantee as relevant) on DD/MM/YYYY at HH:MM:SS based on a digital guarantee file.

The guarantee data
The digital guarantee code: _____

Issuer of the guarantee:
_____ Branch No.: _____
Telephone No. of the guarantee issuer: _____ Fax No. of the guarantee issuer: _____
Address of the guarantee issuer: _____
Street and number: _____ Town: _____ ZIP _____
Name of authorized signatory 1: _____
Name of authorized signatory 2: _____

The guarantee recipient:
_____
The obligees (hereinafter jointly and/or severally: the "Obligee"):

Obligee identifier	Name of the Obligee
_____	_____

Subject of the guarantee:
Public Tender No. - XX

Sums and dates
The guarantee sum _____ new Israeli shekels.
Linkage: _____ Base date for linkage: _____
The guarantee issue date: _____ (this part will be completed by the issuer) Guarantee expiration date: _____

Wording of the undertaking
The guarantee issuer hereby guarantees towards the guarantee recipient, for the Obligee, the settlement of any amount that the guarantee recipient will demand from the guarantee issuer in relation to the subject of the guarantee, which will not exceed the guarantee sum amount. The guarantee issuer hereby undertakes to pay the guarantee recipient the said sum within the number of days for invocation prescribed in the guarantee from the date of the guarantee recipient's demand, without the guarantee recipient being required to explain its demand or first demand the settlement of the sum from the Obligee.

In the case of such a demand, the guarantee issuer will not assert towards the guarantee recipient any allegation of defense that it or the Obligee may have, and will not subject the payment to any condition or delay it for any reason, including for settling the said sum from the Obligee.
This guarantee may not be transferred or endorsed.
This guarantee may be invoked in installments, to the effect that its partial invocation will not invalidate it for the rest of the guarantee sum that has not been invoked, except that the total payment under this guarantee is not to exceed the guarantee amount.

The provisions of Israeli law only will apply to this guarantee.

Appendix B4 – Insurance Requirements

Insurance Requirements

A. The Supplier and/or its representation office in Israel, if there will be one (hereinafter in this section: the "**Representation Office**") will execute all of the insurances set forth herein, jointly or severally, to their own benefit and to the benefit of the State of Israel – the Ministry of Health, including all of the coverages and conditions required below, the limits of liability being not less than those stated below:

1. **Employers' liability insurance [relevant to a Supplier registered in Israel only and/or to the Representation Office]**

   A. The Supplier and/or the Representation Office will insure their statutory liability under the Civil Wrongs Ordinance (New Version) and/or the Liability for Defective Products Law 5740-1980 towards their employees through employers' liability insurance throughout the State of Israel and the held territories.

   B. The limit of liability will not be less than NIS 20,000,000 per employee, per case and for the insurance period.

   C. The insurance will be expanded to cover the liability of the insured towards contractors, subcontractors and their employees if it will be considered as their employer.

   D. The insurance will be expanded to cover the State of Israel – the Ministry of Health, if it is asserted for the occurrence of any work accident / occupational disease that they bear any employer's liability towards any of the employees of the Supplier, contractors, subcontractors in its service.

2. **Limit of liability towards third parties [relevant to a Supplier registered in Israel only and/or to the Representation Office]**

   A. The Supplier and/or the Representation Office will insure their statutory liability under the states of the State of Israel through third party liability insurance for physical injury and

property damage (including consequential damage) for their activity throughout the State of Israel and the held territories.

B. The limit of liability will not be less than NIS 4,000,000 per case and for the insurance period.

C. The policy will include a cross liability clause.

~~D. Any qualification / exception for property that is not owned by the Supplier but which is under its control, possession and supervision will be cancelled [in relation to a Supplier that performs on prem implementation as a decentralized system (separate for each hospital) only].~~

D. Removed.

~~E. Any qualification / exception in relation to property referring to the property of the State of Israel, the supplier or any person in the service thereof who are working or who worked on it directly will be cancelled [in relation to a Supplier that performs on prem implementation as a decentralized system (separate for each hospital) only].~~

E. Removed.

F. The insurance will be expanded to indemnify the State of Israel – the Ministry of Health, should they be considered as responsible for acts and/or omissions of the Supplier and/or the representation office and any persons acting on their behalf.

3. Combined professional liability and product liability insurance [relevant to the Supplier (whether registered in Israel or not registered in Israel and/or the Representation Office]

COMBINED PRODUCTS LIABILITY AND PROFESSIONAL INDEMNITY POLICY FOR THE SOFTWARE AND HARDWARE INDUSTRY.

or

ELECTRONIC PRODUCTS AND SERVICES ERRORS OR OMISSIONS AND PRODUCTS LIABILITY INSURANCE

or

Another text for combined professional liability and product liability insurance for the high-tech sector / computer field as follows: _____ (**subject to Inbal's examination and discretion).**

A. The Supplier and/or the representation office will insure their liability for providing services for procurement, adjustment, testing, installation, instructing on, deployment and maintenance of the LIMS laboratory management system at governmental medical centers for the Ministry of Health, in accordance with the agreement with the State of Israel – the Ministry of Health, by combined professional liability and product liability insurance.

B. The policy will cover the liability of the insurance executor, its employees and agents acting on its behalf:

1. In relation to a professional act or omission – coverage for breach of a professional duty, omissions error, neglect and negligence.
2. Its liability from a defect in a product – coverage for damage sustained in relation to products that have been manufactured, developed, assembled, repaired, supplied, sold, distributed or handled in any other way by the Supplier or a delegate thereof.
3. Activity of the insurance executor, its employees and all agents acting on its behalf including inter alia construction, upgrade, maintenance, characterization, application, testing, instructing and technical support services for the Ministry of Health.

C. The limits of liability will not be less than NIS 20,000,000 per case and per insurance period, but in relation to insurance that will cover the liability of the Representation Office only, the limit of liability will not be less than NIS 4,000,000 per case and per insurance period.

D. The policy will include the following expansions:

1) The disclosure period of at least ~~12~~ 6 months.
2) Cross liability – however, the coverage will not apply to claims of the insurance executor towards the State of Israel – the Ministry of Health.
3) Fraud and dishonesty of employees.
4) Loss of documents, including loss of use and/or delaying due to an insurance case.
5) Invasion of privacy.

E. The jurisdiction and territorial boundaries clause will include the State of Israel, if the Supplier is not registered in Israel.

F. The insurance will be expanded to indemnify the State of Israel – the Ministry of Health, for their liability for damage owing to a defect in products that were supplied, maintained, repaired, upgraded or serviced for the State of Israel – the Ministry of Health, by the insurance executor and all persons acting on its behalf and/or to the extent that they are considered liable for the acts and/or omissions of the insurance executor and they are acting on its behalf.

2. General

Each insurance policy required above will include the following conditions:

1) The State of Israel – the Ministry of Health will be added to the name of the insured as additional insurers, subject to the indemnification expansions above.

2) In any case of an adverse change in or cancellation of the insurance by one of the parties, these will have no effect unless announced 60 days in advance in writing to the accountant of the Ministry of Health.

3) The insurer waives any right of subrogation, claim, participation or recourse towards the State of Israel – the Ministry of Health, as long as the waiver will not inure to the benefit of a person who has caused damage out of malicious intent.

4) The Supplier is exclusively responsible towards the insurer for payment of the insurance fees for all policies and for fulfilling all duties imposed on the insured according to the conditions of the policies.

5) The deductibles specified in each policy will be borne exclusively by the Supplier.

6) Any clause in the insurance policies that expropriates or reduces in any way the liability of the insurer when there is another insurance will not be applied towards the State of Israel and the insurance will be presumed as primary insurance that qualifies for all rights according to the insurance.

7) The coverage conditions of these policies will not be less than the norm according to the conditions of "BIT" version policies (except for combined professional liability and product liability insurance) subject to the expansion of the coverages as set forth above.

8) Any exclusion of intent and/or gross negligence will be canceled.

B. The Supplier warrants on its own behalf and that of its Representation Office that throughout the period of the contractual engagement with the State of Israel – the Ministry of Health and as long as its liability exists, they will keep the insurance policies in effect. The Supplier warrants that the insurance policies will be renewed each insurance period, as long as the contract with the State of Israel – the Ministry of Health is in effect.

C. A confirmation of execution of the insurances signed by an insurer will be produced by the Supplier to the Ministry of Health by the time of signing the contract. The Supplier undertakes to show the confirmation signed with the signature of the insurer about the renewal of the policies to the Ministry of Health seven days before the end of the insurance period at the latest.

D. It is hereby clarified that the insurance confirmations that will be shown are not intended to reduce and/or derogate from the undertakings of the Supplier and/or the Representation Office to execute the insurances according to the insurance clauses set forth above, and for the removal of doubt, the binding insurance requirements are according to the foregoing. The Supplier is required to study and fulfill these requirements and if necessary seek assistance from insurance people on its behalf to fulfill the requirements and implement them in the insurances as required.

E. The State of Israel – the Ministry of Health, reserves the right to receive from the Supplier at any time copies of the policies, in part or in full, in the case of discovery of circumstances that may lead to a claim under the policies and/or for it to be able to examine the Supplier's fulfillment of these clauses and/or for any other reason, and the Supplier will forward the policy copies in part or in full as set forth immediately upon receiving the demand. The Supplier undertakes to make any modification or correction that will be required to adapt the policies to the undertakings according to the insurance provisions above. It is agreed that the Supplier will be allowed to delete from the said insurance policies secret business and/or commercial information that is not relevant to this engagement.

F. The Supplier represents and warrants that the right of the State of Israel – the Ministry of Health to conduct the check and demand the changes as set forth above do not impose on the State of Israel – the Ministry of Health or any delegates thereof any duty or liability in relation to the said insurance policies / insurance confirmations, their nature, scope and validity, or for their absence, and do not derogate from any duty that is imposed on the Supplier for the Agreement, whether adjustments have been required or not, whether checked or not.

G. For the removal of doubt, it is hereby agreed that the insurances requiring limits of liability and coverage conditions are considered to be a minimal demand imposed on the Supplier and do not constitute a confirmation of the State of Israel or any delegate thereof in relation to the scope and size of the insurance risk, and it must examine its exposure and establish the insurances that are necessary for it and for the Representation Office, including the scope of the coverages and the limits of liability and insurance period accordingly.

H. The foregoing in the insurance clauses does not exempt the Supplier and/or the Representation Office from any statutory or contractual duty applying to them and the foregoing is not to be interpreted as a waiver by the State of Israel – the Ministry of Health of any right or relief granted thereto by any statute or this contract.

I. Failure to meet the conditions of these insurance clauses constitutes a fundamental breach of the contract.

Appendix B5 - Information Security

Information and Cyber Security Appendix to the Tender

Disclaimer:
The attached Security Appendix is a general document applicable to various types of tenders, including but not limited to hardware and software supply, hardware-only, SaaS cloud services, on-premises installations, and more. The supplier is required to respond to or address the relevant sections applicable to the current tender. Sections that are not applicable should be marked as "Not Relevant."

1. General

1.1. This document contains a collection of information security requirements for an engagement with the Supplier.

1.2. Compliance with the provisions of this document is a critical condition for engagement with the Supplier and must meet the information and cyber security requirements of the Medical Centers Division within the Health Division (the "Division").

2. Goal

Defining a required information security level as a condition to provision of the services in accordance with the needs of the Division.

3. Definitions and terms

3.1. **Information:** a knowledge item, document, correspondence, plan, figure, model, opinion, conclusion or anything else related and/or pertaining directly or indirectly to the provision of the services, including information relating to the intimacy of the employees of the Division or the citizen, in writing, orally and/or in any other form or manner of keeping knowledge items electrically and/or electronically and/or optically and/or magnetically and/or otherwise, which are related and/or pertain to the provision of the services, which is not in the public domain.

• Integrity of information – ensuring that data remains unchanged from its source and is not modified, delivered, or destroyed without lawful permission.
.
• Confidentiality of information– denial of exposure of the information to unauthorized parties
• Availability of the information – maintaining access to the information continuously
• Protected information – such as – data on a person's personality, intimacy of his personality, health condition, economic status, vocational training, opinions and belief.

3.2. **The Protection of Privacy Law**: the Protection of Privacy law, 5741-1981 -

3.3. **The Protection of Privacy Regulations**: the Protection of Privacy Regulations, 5741-1981 – the Protection of Privacy Regulations (Information security), 5777-2017, directions of the Privacy Protection Authority and any future regulations that will be enacted and future directions that will be published in relation to protection of privacy and information security.

3.4. **Database:** a collection of information data held using a magnetic or optic means (including a computer) and intended for digital processing.

Supplier-side Information Security Officer: The Supplier will designate a contact person with relevant expertise, preferably familiar with the current landscape of cyber threats, who will serve as the information security focal point for implementing the directives in this document.

Formatted: Font: Bold, Complex Script Font: Bold

3.5. **"The information assets:** any information, databases, other data item or equipment of the Division, which is being used for the activity of the database for operating the Tender (if any).

3.6. **Technological infrastructures:** all technological infrastructures used for processing and displaying of the information of the Division, including inter alia: servers, desktop and laptop computers, communication equipment, information security equipment and more.

3.7. **Database users:**

3.7.1. Any functionary of the Supplier, which is required owing to his function to use information that has been accumulated in the Division's databases that are kept on the premises of the Supplier, or to which the Supplier has access.

3.7.2. Functionaries in the Division who receive within their duty reports and information produced from databases of the Division that are kept on the premises of the Supplier or that have access thereto.

3.7.3. Contiguous (third party) systems using information contained in the Division's databases and possessed by the Supplier.

3.8. **Physical security:** the physical means required to protect computer equipment, to access information of the Division and for the survivability of the computer systems containing the databases.

3.9. **Mobile device:** a computer designed for mobile use, including a mobile phone as defined in the Communication Law (Telecommunication and Services) 5742-1982 and/or another medium used for storage of computer material / information.

3.10. **Information classification:** providing a definition of sensitivity for information and accordingly the need to compartmentalize it, based on the principles defined by the Division. Threat to information – any event that compromises the confidentiality, integrity, or availability of the Division's information

3.11. **Information security:** protection of Confidentiality, integrity and availability of the information, protection of the information from exposure, use or copying without lawful permission.

3.12. **Information systems security incident / cyber incident**: an action that is performed maliciously or inadvertently that may compromise the availability, reliability and Confidentiality of the information and/or office computer equipment at various levels and

result in the incapacitation of systems, intentional disruption of data or exposure of data to unauthorized parties.

3.13. **Authentication mechanism:** a means used to verify the identity of a person or system when attempting to log in and confirming the performance of actions on their part to information systems.

3.14. **Unique identification:** a unique value that identifies a person purporting to own the means of identification.

3.15. **Strong authentication:** an identification means based on at least two of the following items:

3.15.1. **Something You Are** – biometric identification, a unique physiological attribute of the user

3.15.2. **Something You Have** – an item possessed by the users

3.15.3. **Something You Know** – a password

3.16. **Cryptography**: Encryption – the process of converting information into a secure format using algorithms, ensuring that only authorized parties can access the information. The main purposes of cryptography are to maintain the Confidentiality and reliability of the information, provide a prevention of repudiation solution for actions and providing a mechanism for verifying the identity of users.

3.17. **Encryption:** use of scientific tools and algorithms for protection of information. The main purposes of cryptography are maintaining the Confidentiality and reliability of the information, provide a prevention of repudiation solution for actions and provide a solution for verifying the identity of users. Encryption may be performed using an element (software), on a server or hardware element or in another way.

3.18. **Firewall**: an element (software on a server or hardware element) that controls incoming or outgoing traffic to and from a communication network according to a defined security policy.

3.19. **Vulnerability**: a weakness in a system that may lead to materialization of a threat.

3.20. **Log:** a record of events or transactions within a system, often used for auditing, monitoring, and forensic purposes, documenting actions such as access, changes, and error.

3.21. **Yahav:** a unit operating within the Government ICT Authority for cyber protection in the Government in the National Digital Agency. The unit was established according to Government Resolution 2443 to promote national regulation and Government leadership in cyber protection.

3.22. **Outsourcing:** the use of outsourcing services means taking out of the organization, or persons who are not employees of the organization performing actions and processes that are usually performed by the Division.

3.23. **Supplier:** a party that has been declared as a winner of a tender and a service provider (including consultation) or goods supplier to the Division.

3.24. **Major / critical supplier:** a supplier providing services such as: support and/or maintenance of technological infrastructures and/or information systems, storage of sensitive data outside the Division, technological outsourcing services or in the case of compromising the Supplier having potential to cause major damage to the Division.

3.25. **Authorized suppliers:** suppliers that have gone through a risk review process through an examiner and have accessed through the examiner a certification body that is authorized to issue the Supplier an “approved supplier” certificate.

4. Methodology

4.1. The Supplier will appoint an Information and Cyber Security Officer responsible for implementing all aspects of information security across systems and processes.

4.2. The Supplier undertakes to implement the organizational cyber protection doctrine as outlined by the National Cyber Directorate, ensuring alignment with its guidelines and best practices (the "Protection Doctrine") in a manner corresponding with its activity, its size and complexity, while managing the risk as a function of likelihood and impact. The work plans for implementing the reviews according to the Protection Doctrine will be approved by the Division.

4.3. The text in this document does not exempt the Supplier from or reduce its responsibility for to all statutory provisions pertaining to managing databases and safeguarding individual privacy and intimacy and any other law relevant to the matter.
This document does not replace any specific instructions or directives from any party with regard to the recipient of the information. However, it establishes the foundational expectations that the Division requires the Supplier to adhere to when receiving information.

4.4. The failure to implement the principles stated in this document, in part or in full, may result in termination of the engagement at the Division's professional discretion.

5. Compliance with standards

5.1. To the extent required, the Supplier will fulfill the regulatory requirements set forth below (at the time of submitting the bids for the tender or at a later time that the Division will pronounce):

5.1.1. The relevant ISO27001 standard – the Subsection must produce a certification document proving compliance with the ISO27001 standard from the ANAB certification body, which is responsible for performing a certification audit under international IQC accreditation, such as: the Standards Institution of Israel, ANSI (national accreditation board), etc. The certification will be produced to the Division within 120 days of the time of signing the engagement contract.

5.1.2. In the case of medical information, the Supplier undertakes to comply with the medical information security and privacy in organizations standard according to ISO 27799.

5.1.3. The Supplier undertakes to comply with the ISO27017 standard for working in the cloud environment if there is any work in that environment.

5.1.4. The Supplier undertakes to comply with the ISO27018 privacy production standard for work in the cloud environment if privacy protection aspects in that environment apply.

5.1.5. The Supplier guarantees that if it possesses records containing information about international credit card companies, it will comply with all relevant PCI-DSS standards as applicable.

6. Classification and mapping of the information

6.1. The Supplier will act according to the information classification defined by the Division. The service will be characterized according to this classification.

7. Characterization of the proposed service

7.1. The Supplier must describe and attach a document describing the information security policy of the proposed service.

7.2. The breakdown is to include inter alia the following sections:

- General – a general explanation on the company and the cooperation with the Division.
- The geographic location in which the company's technological infrastructures are located through which the service to the Division is supposed to be provided.
- Physical security – for the project environment.
- Structure tree and breakdown of relevant functionaries (CEO, CIO, information security manager, etc.).
- Breakdown of information security training of functionaries in the information security field.
- Description of the business process.
- Description of the architecture of the proposed system.
- Information security controls used by the system
- Backup and DR procedures
- The manner of integration of information security in the SDLC (system lifecycle) process
- Organizational processes for reducing risks and coping with threats.
- Presence and evaluation of compliance with standardization and laws and breakdown of certifications for information security standards such as: ISO27017, ISO27001.
- Manner of identification of and response to events.
- Evaluation of employees and reliability tests.
- Performing periodical penetration tests (method, etc.).
- Implementation of monitoring and review mechanisms.
- Manner of dealing with the issue of user management, authentication and authorization management.
- Identification of weaknesses and installation of patches.
- Information security in communication (breakdown of required products).
- Check of interfaces.
- Manner of protection of information at rest and on the move.
- Additional information security products at the infrastructure level and/or at the applicative level.
- If the system supplier uses an IT infrastructure of another supplier, it must state this and attach a document describing how the assignment of responsibility between it and the additional infrastructure supplier occurs and what means it uses to protect the information against damage at the infrastructure level and have this approved with the information security and cyber unit.

8. Safeguarding Confidentiality and privacy

8.1. The Supplier undertakes to follow the provisions of the Computers Law, 5755-1995, the information security statutes, including the Protection of Privacy Law, 5741-1981 and the Protection of Privacy Regulations (Information security) 5777

8.2. The Supplier undertakes to follow all information security instructions about safeguarding of information as forwarded by the Division.

8.3. The Supplier will see to securing all material that reaches it within the performance of its obligations hereunder and will be responsible towards the Division for all of the information that is forwarded to or through it, including reports, personal data, email correspondences, files, documents, drawings and the like according to the directions that will be forwarded by the Division.

8.4. The Supplier is responsible for seeing to the confidentiality, reliability and availability of the information of the Division in its possession.

8.5. The Supplier will be responsible for any bypass or attempted bypass of security mechanisms and access controls of various infrastructures, which will be carried out by its employees.

8.6. During an information security / cyber incident or an adverse event on the Supplier's premises, including an incident in which there is suspicion of leak of the Division's information, the Supplier undertakes to notify the division's contact person ~~immediately~~no later then 24 hours, ~~no later than the workday on which~~ from the time the incident occurred and was brought to the Supplier's knowledge.

8.7. The Supplier undertakes to cooperate with the Division in any adverse event involving an employee of the Supplier, or when there is suspicion of involvement that directly or indirectly impacts the security of the information systems of the division, any violation or suspected violation of laws or regulations or information security procedures including in investigation of events or suspicions of information security irregularities or a leak of the Division's information to unauthorized parties.

8.8. If project-related documents are transferred in encrypted form, they must be stored on the Supplier's premises in their encrypted state.

8.9. "Restricted" information will be accessible to the Supplier's employees on a need to know basis.

8.10. Preparing copies for work purposes at the Supplier's premises will be done as necessary only and their distribution will be to employees of the Supplier required to keep these copies only.

8.11. The Supplier undertakes to appoint an information security officer on its part, who will be responsible for dealing with the databases kept by the Supplier and implementation of the directions appearing in this document.

8.12. The Supplier will sign a nondisclosure agreement, in a form attached to the tender, and will have this NDA signed by its employees and/or agents that will have access to a database of the Division or to information inside it within the engagement.
If the Supplier engages with any third party that impacts the engagement between the Supplier and the Division or the implementation of directives outlined herein, the Supplier must seek approval from the Ministry, follow its guidance, and inform the third party of their obligations under this document. All such engagements must be approved by the Division

8.13. The Division is allowed to perform process and technological control on the Supplier's side after arranging with it at least ~~a~~ 2 weeks before performing the review. The Supplier undertakes to cooperate with the representatives of the Division to that end. The Supplier will provide the Division the details required for the review: functionaries relevant to information security, details of the Suppliers of critical system and service providers (cloud supplier, Internet service provider, website hosting provider, etc.). The Supplier will update the Division on any change in these details.

9. Use, maintenance and management of databases

9.1. The Supplier warrants that any access by it or a delegate thereof to information and the database will be performed only in accordance with the instructions of the Division and for the purposes defined for it by the Division within the engagement.

9.2. The Supplier warrants that it or an agent thereof will not transfer information or part of information out of the databases of the Division in its possession or to which it has access to any third party without the advance written approval of the Division.

9.3. The Supplier undertakes to prevent saving of sensitive data locally on devices of the system users. In exceptional cases, explicit advance written approval from the Division must be obtained.

10. Risk identification and management

10.1. The Supplier must detail a performance plan for managing and identifying information security risks at all stages of the project.

10.2. The Supplier will perform periodical information and cyber security risk reviews for security products, systems, infrastructures and key processes. A risk review will be conducted will not be less than once every 36 months and will be validated at least once every 18 months. The reviews will be done by an outside company specializing in information and cyber security and that is not related to the Supplier or to the entities that have developed the systems. The findings of the surveys will be shown to the Division's information and cyber security unit and a work plan for corrections will be formed according to prioritization of the Division. The Supplier undertakes to act according to the work plan for correcting information security risks that have been discovered.

10.3. The Supplier must obtain Division approval before making any modifications to the system architecture or service provision methods.

10.4. The Supplier undertakes to offer alternative controls to the requirements set forth in this document. These controls will be implemented after getting advance written approval from the information security entities in the division.

10.5. The Supplier will show an analysis of possible courses of action (MOs) for attacking the project's information security infrastructures including possible solutions for coping with the different attack types.

11. Information security in the human resources and employees plane

11.1. The Supplier warrants that all of its employees and/or delegates that will have access to the Ministry's databases and/or who will be employed within the Supplier's engagement with the Division will have suitable training as required in the tender and engagement documents. A background verification check of each candidate for employment as an employee of the Supplier, a delegate thereof or any third party user will be done by the Supplier as required by law and according to all relevant ethics rules, and their scope will correspond with the requirements of the Division for the classification of the information that will be accessible to them and the expected risks.

11.2. The Supplier will be responsible towards the Division for any activity of its employees and/or delegates within the engagement.

11.3. The Supplier warrants that all of its employees and/or delegates and/or third party users understand all of the responsibility imposed on them in relation to the information and its protection and that they are suitable for their intended functions. The Supplier must reduce risks of theft, fraud and misuse of access to the Division's information by taking reasonable, acceptable protective measures (such as security cameras, documentation of access, etc.) without derogating from the provisions of this appendix in relation to physical and environmental security.

11.4. The Supplier must perform information security awareness training for its employees in an employee's field of occupation at a frequency of once a year and document it.

11.5. The Supplier undertakes to prevent cases of its employees and/or delegates attempting to access databases for which they have not received authorization.

11.6. The Supplier warrants that the functions and responsibilities of employees of the Supplier and/or a delegate thereof and/or third party users pertaining to security will be defined and documented by the Supplier according to the organization's information security policy.

11.7. A contract signed with new employees will include attention to the employee's responsibility in relation to information security aspects and will be provided with a nondisclosure agreement.

11.8. A contract of the Supplier with personnel / recruitment companies or with companies providing outsourcing services will include attention in relation to checks performed in employee hiring processes, information security during the employment of employees and increasing their awareness. The Supplier's information security procedures will define actions that must be performed to safeguard the Division's information assets.

11.9. The Supplier must define procedures, reviews and additional actions that are intended to prevent leak of information from its employees who have access to information of the Division.

11.10. Employees (including workers outside of the organization) who conclude their employment in the organization, whether at their own initiative or that of the employer, will have their information access authorizations blocked (whether to information systems or to physical means).

11.11. The Supplier will make sure that at the conclusion of employment, the employees will retain no information assets of the organization.

11.12. The Supplier will define the manner of dealing with employees in information security aspects for the period between the notice of leaving and the conclusion of employment. Requirements on access control, working on systems and documents, etc., must be defined at least.

12. Physical and environmental security

12.1. The Supplier undertakes to protect the work areas in which a connection is made to the Division including work of systems / databases of the Division.
12.2. The Supplier warrants that access to areas in which there is information and/or databases and communication cupboards will be documented and controlled in a manner allowing for verifying the identity of the person accessing the said equipment.
12.3. The Supplier undertakes to develop and implement physical security protocols for working in the designated areas according to physical security best practices for development software companies~~.~~
12.4. Securing equipment and paperwork – the Supplier will make sure that the following steps are taken in relation to securing equipment and paperwork:
12.4.1. Equipment containing sensitive information and intended for destruction or maintenance or that has been delivered to a party outside the Supplier does not contain information on customers of the Division.
12.4.2. A memory medium that contained information on the customers of the Division will be taken out of the Supplier's premises for maintenance purposes only after sufficient means have been taken to delete the information in a manner precluding restoration of the information using technological means including after deletion of the information.
12.4.3. Sensitive media that have no use will be shredded or destroyed.
12.4.4. Paperwork arriving for scanning will be secured adequately, including in the archiving and destruction process.

13. Logical security

13.1. The Supplier undertakes to implement adequate security means to prevent intentional or accidental penetration of the infrastructure and communication system or systems (including by remote connection). The control means must be shown to the information and cyber security before their implementation and prior written approval of the control means chosen obtained.
The Supplier warrants that all information security means will undergo hardening according to the manufacturer's recommendations.
13.2. The Supplier undertakes to update regularly the various systems, including those that connect to the Division, to prevent exploitation of information security weaknesses.
13.3. Updates at the critical hardware level will be installed within 3 days, updates of medium/low level will be installed at a reasonable time, which will be determined by the Division. After publication of a notice by the manufacturer / Ministry / other authorized governmental entity.

14. Documentation and review

14.1. The Supplier undertakes to manage an automatic documentation mechanism that will allow for review and inspection of all technological systems, including databases of the Division. Including infrastructure protection system management interfaces.

14.2. The Supplier will apply audit mechanisms to interfaces and ~~key~~ provided systems, for identification and warning of irregular security incidents~~/, on the side of internal users and external users alike~~. The solution to the requirement is to be ~~attached~~ specified ~~to~~ in the answer booklet~~.~~

14.3. The Supplier must document any incident that compromises the integrity, Confidentiality and availability of the information, the solution to the requirement must be attached.

14.4. Any security incident will be investigated and studied and an incident report describing the causes of the incident and the ways it was dealt with will be produced. The Supplier will provide directions to follow in order to reduce the chance of a similar incident occurring. In addition, the Supplier will forward the incident report for reading by the Division's information and cyber security unit.

14.5. The Supplier must prepare instructions for coping with information security incidents that refer to the severity of the incident and the sensitivity level of the information. These instructions will include comments on immediate steps required for dealing with an incident such as reporting to the Division, cancelling authorizations, etc. An example of a requirement must be attached to an answer.

14.6. The Supplier will integrate a solution for documenting activity that will be defined as critical in the system, activity that appears to be irregular (such as activity in the database and/or operating system) and activity or attempts to perform actions that directly contravene the system's defined policy. In addition, the system must provide suitable tools for saving these files and ability to report to the appropriate functionaries so that they may deal with warnings.

14.7. The mechanism of controlling the system will allow for tracking of the following events:

- Login/ Logout. Use of the authentication mechanism
- Failed system login attempt
- Attempts to access information without access authorizations
- Applicative events that are defined as requiring control by a special set of tools for this purpose
- Deletion of objectives in the system
- Activities that are performed by parties with high authorization
- Administration actions (user management, adding and removing services, etc.)
- Operational errors (system failure, software error messages, etc.)

14.8. For any event that is defined as requiring review, the following details will be kept:

- Date and time
- Source of performing the action, for example: IP address
- User Name
- Incident type
- Success or failure of the incident
- Identification of the object on which the action is being performed, for example: filename

- Description of the action (what was done): for each type of event, provide relevant content. For example: update of a record, attempt to access a record, deleting a user, shutting down a system, etc.
- The messages must be reliable, full and clear.
- The Supplier must specify the abilities of the system to export the data to the SIEM system
- The control mechanism must interface with the reports mechanism and supply a high level of reports, information profiling, etc.
- The control apparatus must be adequately secured. Only authorized users will get access to it. In particular, attention must be paid to access control for the ability to load up and remove the control mechanism.

14.9. The Supplier warrants that access documentation will be kept on servers that are separate from the database.
14.10. The Supplier warrants that the control mechanism will not allow for cancellation or changing of its operation. The control mechanism will identify changes or cancellations in its operation and will distribute warnings to the information security officer of the Supplier and the information and cyber security unit of the Division.
14.11. The Supplier undertakes to forward to the Division periodical reports and upon demand in relation to the manner of management of information owned by the Division and during a cyber incident.
14.12. The~~A critical~~ supplier undertakes to submit to the Division each year an external audit report signed by a qualified professional (any party accompanying organizations for information security certifications).
14.13. The Supplier undertakes to report ~~immediately~~ within 24 hours, to the information security and cyber unit in the division any case of a cyber incident, fear of an information leak from the database or irregular use of the authorization provided.
14.14. The Supplier undertakes to keep the recording data of the control mechanism for 24 months at least.

15. User Management and Authorizations Management

15.1. The Supplier warrants that access to the information systems and/or databases will be on a need-to-know basis and access beyond necessity for performing a function as defined by the Division and in accordance with the provisions of the tender will not be permitted.
15.2. The Supplier undertakes to see to compartmentalized access based on role definitions.
15.3. The Supplier undertakes to keep an updated record of the functionaries and the access defined for each function.
15.4. The Supplier undertakes to remove authorizations of functionaries whose function has ended or for whom there is no need for information for which they have received authorization.
15.5. The Supplier undertakes to see to the appropriate controls so that no unauthorized access to databases will occur.
The Supplier ensures that network and administrative service management remotely will be authenticated using two-factor authentication (2FA)

15.6. The system will identify the users by the authentication array
15.7. Priority will be given to interfacing to an enterprise Active Director. If not, a password policy that will include at least the following parameters will be defined:
  15.7.1. Password strength – at least 8 characters combining digits and letters
  15.7.2. Number of wrong attempts until lockout – 3 attempts
  15.7.3. Saving of password history – up to 5 passwords back
  15.7.4. Frequency of changing password – once every 3 months
15.8. The system will disconnect a user who has logged into an information system after 10 minutes of inactivity

16. Communication elements security

16.1. The Supplier warrants that information systems and databases of the Division will not be connected to the Internet environment, unless it has received advance written permission from the Division to do so.
16.2. If the Supplier has received permission and has connected the information systems and/or the databases to a public network or to the Internet, the Supplier undertakes to take suitable protective measures to prevent damage, hacking, contamination or mutilation of databases. The Supplier's proposal for coping with these threats is to be elaborated and the list of controls and means providing an answer to the requirement is to be attached to the answer.
16.3. The Supplier warrants that the transfer of the information inside the communication network, on a public network or on the Internet, will be done using commonly accepted encryption methods using advanced protocols.
16.4. The communication equipment (FW switches, routers, etc.) must be hardened in accordance with the manufacturer's policy and undergo firmware updates.
16.5. The Supplier will show the division the secure solution for transfer of information by cellular communication in the case of it choosing to implement it for getting the Division's approval.

17. End point Security

17.1. Saving of sensitive information on a remote user station that has not been adapted to the policy of this document is strictly prohibited.
17.2. The computers of the Supplier from which it is possible to access information of the Division and its systems will be equipped with an updated operating system and EDR programs (Windows 10 and higher) for protection against malicious code (viruses, worms, trojan horses and other spyware types).
17.3. The Supplier undertakes to install a content filtration element that will prevent the entry of code into the Supplier's network during Internet browsing and email use, if approved by the Division (content filtering).
17.4. The Supplier undertakes not to save information of the division on laptop computers and/or smartphones.

17.5. The transfer of information / software / updates to the Division's network will be done after a sanitization process.
17.6. The environment that will be configured at the Supplier's premises for dealing with information of the Division will be separated from the Supplier's work environment by segmentation or by full physical or logical separation.
17.7. The connection to the Division's information system will be in accordance with the Division's directions.

18. Use of Portable memory devices

18.1. The Supplier undertakes not to take information elements out to Portable memory devices except for backing up the information as established by the Division.
18.2. If the Supplier is required, for its activity, to load up information elements for backup purposes, the Supplier undertakes to get advance approval from the information and cyber security division in the Division and to take adequate protective means to ensure the integrity, Confidentiality and availability of the information.
18.3. In a database that can be connected to remotely via the Internet for management purposes, The Supplier undertakes to use strong authentication, specifically Multi-Factor Authentication (MFA).

19. Backup, restoration and recovery

19.1. Information of the Division that is in the Supplier's systems will be regularly backed up according to the policy established by the Division.
19.2. The Supplier undertakes to make secure backups of the information that it has accumulated.
19.3. The Supplier undertakes to store the backup media in a manner that will ensure the integrity of the information and will ensure the possibility of restoring the information in the case of loss or destruction.
19.4. If third party suppliers are used for storing backups, this must be approved before starting work with the Division.
19.5. The Supplier undertakes to perform sample restorations of the backup media on its infrastructures for checking recovery in accordance with the work plan.
19.6. After ending the sample restoration, the Supplier undertakes to delete the restored information.
19.7. The Supplier warrants that the restoration will be done only with the approval of the Division's information security manager.
19.8. The Supplier warrants that if restoration has been done, all restoration processes will be documented including the identity of the restorer.
19.9. The Supplier undertakes to prevent mixing of information of different classifications during restoration.

20. Software development

20.1.In relation to the development of software, the Supplier must meet the best practice direction for secure development ~~such as the Yahav 5.13 direction~~ such as OWASP (Open Web Application Security Project), NIST (National Institute of Standards and Technology), CIS (Center for Internet Security), **ISO/IEC 27034-1:** Provides international standards for application security, ISO - International Organization for Standardization, SANS Secure Coding Practices,

~~20.1.~~20.2. . In addition, the Supplier must apply the following emphases:

~~20.1.1.~~20.2.1.The software code will contain only the entries in the documentation provided with the software as negotiated with the Division.

~~20.1.2.~~20.2.2.The software code will be without records of management passwords, backdoors, trojan horses, etc.

~~20.1.3.~~20.2.3.The software will be inspected (code reviewed) thoroughly by independent penetration testers. Bugs that impair the system's information security will be repaired. This vulnerability, if present, will be corrected and reported to the Division.

~~20.1.4.~~20.2.4.The code will be scanned by static / dynamic application security testing. Security flaws that will appear in the scan report will be corrected before being loaded up into the production environment.

~~20.1.5.~~20.2.5.The system will not make code changes in ancillary systems such as n operating system, which impair the general information security level of the Division's computer systems.

~~20.1.6.~~20.2.6.The Supplier warrants that in future versions of the system, no major changes will be made, as opposed to unexpected bugs, which will impair the system's information security level without explicit permission from the Division

21. Work in a cloud environment

21.1.The proposed system will operate in the cloud of the Division and the bidder is required to provide a solution **for the cloud environment according to the Nimbus tender and the requirements for the cloud in the appendix to this tender.**

21.2.It should be clarified that the connection of interfaces to On Prem systems of the Division will be done on a secure medium line that will be approved by the Division.

21.3.The connection of the Supplier to the cloud environment will be done from a controlled, monitored jump server of the Division.

21.4.The Division has an active work environment in the cloud in which many security inputs have been invested.

21.4.1.In the case of the cloud environment that will be defined by the Division being additions / expansions, the relevance to the existing security models is to be shown.

21.4.2.In the case of the cloud environment to be defined by the project being another cloud environment (within Nimbus), the required security elements are to be shown (at all layers) for approval by the information and cyber security unit.

21.5.Architecture and mapping:

Formatted: Left, Left-to-right, Line spacing: single

Formatted: Complex Script Font: 12 pt

Formatted: Not Highlight

Formatted: Font: (Default) Segoe UI, 10.5 pt, Font color: Auto, Complex Script Font: Segoe UI, 10.5 pt

21.5.1. The Supplier will show a full network architecture that includes the required protection elements.

21.5.2. According to the statements in the technologies appendix of this tender and before deployment, mapping of the data flow between all cloud services and the internal computing systems of the Division / other nodes is required, including the information flow configuration from / to cloud services.

21.5.3. The manner of protection of the interfaces is to be shown.

21.6. Information and files:

21.6.1. The Supplier will show the manner of protection of the information in each of its life stages (entering the cloud, transfer between different cloud environments, etc.).

21.6.2. The Supplier will show the manner of dealing with different file types including file validation, sanitation, etc. The solution is to be approved with the information and cyber security unit.

21.7. Organization

21.7.1. The Supplier is to define~~d~~ the organizational units & accounts organization ~~to the extent~~in case that these are not defined in the cloud environment to be chosen.

21.8. Identity and access management:

21.8.1. The Supplier will define with the Divion the user groups, functions and authorizations required.

21.8.2. The management will be managed preferably using the Division's Active Directory

21.8.3. The Supplier will define the access control and security control policy if not defined in the chosen cloud environment.

21.9. Logs / monitoring:

21.9.1. The indication (log files) in the system will be protected against unauthorized access (viewing, modification, deletion) and the option of unauthorized access identification will be maintained. The system will warn of an access / usage attempt exceeding the limits of the authorizations given.

21.9.2. The log data will be transferred for monitoring to the SIEM systems

22. Supply chain

22.1. As part of the bidder's requirements for certification in the Yuval system of the Cyber Directorate for calculation of compliance with local and international standards at the initial stage in filling in the questionnaire

22.2. The winning supplier will be required to fulfill the supply chain requirements according to the criticality level, will undergo verification (inspection) of its compliance with the conditions of the certification section.

22.3. ~~The Supplier will make sure that products and services supporting the Division's processes and vital systems take security means according to common standards in the field and according to the Yahav direction 5.19 – "supply chain", and the information and cyber security unit's direction.~~Section removed.

22.4. Suppliers will be rated according to three risk levels **A – high, B – medium, C – low. The risk levels are derived from the highest criticality level of that supplier, the score being**

derived from the maximum damage potential. For example: a supplier classified as C for some criteria that is at risk level A in one of them will be classified at risk level A. The criticality level is measured according to the scope of communication with the Division (sum of money), the sensitivity of the information and the likelihood of materialization of an incident as a result of the engagement. An accessory table for establishing the rating follows:

Supplier rating	**Expected damage level to the Ministry from the Supplier**	**Scope of engagement of the Ministry with the Supplier**	**Impairment of business continuity**	**Sensitivity of information accessible to the Supplier**	**Likelihood of materialization of an incident as a result of the engagement**
C	Low	Tens of thousands of shekels	Recovery from an incident on the Supplier side will take a few hours	information of low sensitivity level	Low dependence on Cyber. For example, a supplier of office equipment, expert services that do not include information on the customer, without authorization or access to customer systems, etc.
B	Medium	Hundreds of thousands of shekels	Recovery from an incident on the Supplier side will take a few days	information of medium sensitivity	Medium dependence on cyber in the engagement with the Supplier
C	High	More than NIS 1 million	Recovery from an incident on the Supplier side will take a few weeks	Sensitive business information such as patents, commercial secrets, etc.	A ss with high dependence on cyber. For example: a supplier that provides IT services, with remote access authorizations, a major software supplier, possessor of sensitive information in the cloud or systems in the Supplier's environment

22.4.1. Suppliers that have been rated at level A – are responsible for proving a protection level according to suppliers' questionnaire in the Yuval system using a suppliers' examiner / qualified checking party (according to a list of the National Cyber Directorate published on the Internet). Information regarding the Yuval system is attached in a separate file.

22.4.2. Suppliers that have been rated at level B – are responsible for proving a protection level according to suppliers' questionnaire in the Yuval system and attaching the evidence required in the questionnaire.

22.4.3. Suppliers that have been rated at level C are responsible for filling in the Suppliers questionnaire and having an attorney or the company CEO sign a supplier declaration on its compliance with the protection requirements in the questionnaire.

22.5. Before the engagement, the Division will define to the Supplier what its risk level is according to the criteria described and ~~also~~ the Supplier will be given a definition of what actions it must perform to implement the protection level required in accordance with the directions of the National Cyber Directorate.

22.6. In the case of the Supplier being certified according to the directions of the National Cyber directorate as set forth, the winner must show the "approved supplier" certificate and the results of the survey.

22.7. A major supplier (A rated supplier) is required to show an "approved supplier" certificate. The certificate is issued after an audit performed by an enterprise supply chain qualified cyber compatibility examiner. The audit will be conducted according to the National Cyber Directorate suppliers' questionnaire, for all engagement types (broad requirements, software development, information storage / processing in the cloud, remote access) and according to the Supplier's level of involvement in a major engagement.

22.8. Suppliers whose effect on critical processes is lower will be required to answer the National Cyber Directorate suppliers' questionnaire at a proof level of self-assessment or self-assessment with evidence, according to the operator's risk assessment.

22.9. The Supplier is responsible for filling in the following details before the engagement and forwarding them to the Information and Cyber Security Division:

Name of the Supplier	Service / product type	Customer's contact person	Supplier's representative	Service type (system, software, cloud, etc.)

22.10. Once a year validation of the Supplier's protection level will be performed by answering a self-assessment suppliers' questionnaire.

23. Oversight and periodical inspections

23.1. As set forth in Section 9 above (risk identification and management), the Supplier undertakes to perform an information security survey at least once every 36 months and survey validation once every 18 months – a security audit. In addition, the Supplier undertakes to perform every 18 months a penetration test into its own communication network and systems using a third party whose identity has been approved by the Division and to forward the results of the survey and penetration test to the Division's information security manager for inspection.

23.2. The Division is allowed to conduct inspections (through the Ministry's information security department and/or using an external provider employed thereby) at the premises or in the systems of the Supplier (besides those that the information security company that the Supplier will choose will perform) to make sure that the directions of this document are

met and/or for identification of any possible risk to the information of the Division. These inspections may include, at the Division's discretion, the following:

23.2.1. Overall review of work processes and procedures relevant to the Supplier's work with the ~~division~~Directorate;

23.2.2. Implementation of measures for securing the human resource at the Supplier's premises;

23.2.3. Implementation of physical and environmental security measures at the Supplier's premises;

23.2.4. Implementation of logical security measures in the Supplier's premises (including entering the Supplier's systems and/or checking using automated tools on the Supplier's network and systems).

23.2.5. Examination of the strength of the Supplier's information systems from within or outside the Supplier's network by an independent outside party, as defined by the Division (in coordination with and with the consent of the Supplier).

24. End of engagement

24.1. The Division will require that the Supplier delete the information at the end of the engagement, or at any pervious point in time (such as in the case of suspected hacking and/or information leak at the Supplier).

24.2. It must be ensured that arrangements with the Supplier that were established within the engagement agreement are fulfilled. In particular, it is important to make sure that the deletion of the Division's data stored on the Supplier's premises at the end of the engagement between the parties is verified. The following issues, among others, must be examined:

- It must be verified that the Supplier no longer has any access authorizations, authentication methods, or physical and/or logical access to the Ministry's information.
- A supplier working in a cloud environment must make sure that the material and the encryption key are deleted to make sure that remaining material is illegible.
- The Supplier will sign a declaration in which it warrants that no elements pertaining to the system and/or information about the Division are left in its possession and that it will not use any information of the Division to which it has been exposed within the engagement.
- It must be ensured that magnetic media on any equipment used by the Supplier during the engagement with the Division is destroyed (such as: in the case of computers of the Supplier that were used for processing / storage of Division information). In addition, it is necessary to make sure that copies of the files and information of the customer are deleted from the information systems and information assets of suppliers after the engagement is over.
- It must be ensured that the Supplier has no remaining access authorization, authentication means and physical and/or logical access to the Ministry's information.
- It must be ensured that there is a direction on dos and don'ts in relation to announcing details of the project / engagement to third parties.

Appendix B6 - Nondisclosure and No Conflicts of Interest commitment

I, the representative of the Supplier authorized to declare and undertake on behalf of _____(hereinafter: the "**Supplier**") ask to engage with the Division to supply computer / system services, and after I have been warned that I must state the truth and will be liable for the penalties prescribed in the law should I fail to do so, hereby declare and undertake on behalf of the Supplier and any delegate thereof as follows.

1. The Supplier and any delegate thereof undertake to keep completely and absolutely secret any document, knowledge item, information, details and data of any type, including data about the client, its facilities, details of its employees and patients of the medical centers (hereinafter: the "**Information**"), whether the Information reached them as a result of their engagement with the Division or in any other way, directly or indirectly or produced by them in relation to the engagement.

2. The Supplier and any delegate thereof undertake not to transfer, deliver or bring to the knowledge of any person or entity any information that has reached them in relation to executing the engagement, during or incidental to its performance, before its beginning or thereafter.

3. Within this commitment, the Supplier and any delegate thereof undertake not to announce, permit access to, store or retain using any means in a manner allowing access by any third party, directly or indirectly, to the Information or any part thereof, whether on written media or magnetic, electronic or digital media, including on the Internet and on the website of the Supplier or any third party.

4. The Supplier undertakes not to make any use of the Information, directly or indirectly, except as required for executing this Agreement.

5. The undertakings of the Supplier according to this document are for an indefinite period and are a material condition to fulfilling the engagement.

6. The Supplier and any delegate thereof will not make contact with any person in lawful custody besides as necessary for performing the undertakings of the Supplier in the Tender.

7. The Supplier and any delegate thereof are aware that failure to fulfill the undertakings above ostensibly constitutes a violation of Chapter G, Article E, of the Penal Law, 5727-1977, the violator of which is subject to the penalties prescribed in the law.

Name	**Function**	**Signature**

(Do not sign when submitting the bid - the commitment is intended for the Supplier's employee to sign before they start providing the Services to the Division)

I, _____, Identity No. _____, whose function at _____ *[fill in the name of the Supplier]* (hereinafter – the "**Supplier**") is _____, am giving this undertaking in relation to its engagement with the Governmental Medical Centers Division.

1. In this NDA the following terms will have the meaning appearing beside them.

   "**Information**" – any information, know-how, knowledge, document, correspondence, plan, figure, model, opinion, conclusion and anything else like it related to the provision of the services – whether in writing or oral and/or in any form or manner of keeping of knowledge electrically and/or electronically and/or optically and/or magnetically and/or otherwise.

   "Information" or "secret information" will not include information that is in the public domain or that entered the public domain without a breach of the duty of secrecy and/or information that must be disclosed pursuant to any statute or order of a competent authority and/or information that was developed independently without dependence on the secret information and/or information duly received by the Supplier from a third party without breach of a duty of secrecy and/or information that will be created by the bidder / supplier within the provision of the services according to the Agreement that is generic, general and does not contain data and/or information that were forwarded by the Division.

   "**Professional secrets**" – any information that will reach me in relation to the provision of the services, whether received during the provision of the services or thereafter, including but not limited to: information that will be provided by the State of Israel and/or any other entity and/or delegate thereof.

2. I undertake to keep the information and the professional secrets that will reach me due to the Agreement with absolute secrecy and use them only for the purpose of fulfilling my duties under the Agreement.
3. Without prejudice to the foregoing, I undertake not to publish, transfer, announce, deliver or bring to the knowledge of any person the information and the professional secrets that have reached me owing to the Agreement, except for information that is in the public domain or information that must be disclosed by law.

4. There is no conflict of interest between any other activity or other undertaking of mine and the undertakings of the Supplier pursuant to this Agreement.
5. I will refrain from any action that may create a conflict of interest between the discharge of my duty pursuant to the Agreement and the fulfillment of a duty or other undertaking, directly or indirectly.
6. I undertake to inform the Client of any *concern* for conflict of interest between my undertaking according to the Agreement and any other activity of mine.

Name: _____ Signature: _____ Date: _____

Appendix B7 - Undertaking of an Israeli Representation Office for a Supplier whose place of residence is outside of Israel

I _____, Identity No. _____, an authorized signatory at _____ *[fill in the name of the representation office]*, at the address _____, email _____ telephone No. _____ (hereinafter: - the "**Company**") and serving as a _____ in the Company, hereby confirm that the Company is the official Israeli representation office of the Supplier _____, Company No. (international) _____, whose place of residence is _____ (hereinafter: the "**Supplier**").

I am giving this affidavit for the purpose of submitting a bid on behalf of the Supplier within a tender for procurement, adjustment, testing, installation, instructing on, deployment and maintenance of the LIMS laboratory management system at governmental medical centers, No. 110-2024 (hereinafter: the "**Tender**"). I hereby declare and undertake as follows:

1. I confirm that there is an engagement agreement between the Supplier and the company for provision of representation services in Israel.
2. I confirm that the Company will submit the bid for this Tender on behalf of the Supplier .
3. I confirm that the address of the Company will serve as the address of the Supplier for sending messages and will constitute an address for sending processes of court, in the period of submitting the bids for the Tender and throughout the Engagement Period.
4. The Company and the Supplier are aware that a binding condition for submitting the bid is for the Supplier to engage with the Company as its representative throughout the engagement period too and not just for submitting the bid.
5. I undertake to inform the Governmental Medical Centers Division in writing 90 days in advance in the case of the engagement between the Company and the Supplier ending.

_____	_____	_____
Date	Full name of the signer on behalf of the Company	Signature and stamp of the Company

Attorney Confirmation of the Undertaking of the Company above

I hereby confirm that the declaration above was duly signed by the authorized signatories of the Company.

Date	Full name of the attorney + license No.	Signature and stamp of attorney