**Division of the Accountant General—  
Government Procurement Administration**

**Central Tender No. 05-2022**

**Specific Invitation for the Provision   
of SSE (Secure Service Edge) Products   
and Related Services**

**Version 1, October 2023**

**1. Rules of the Specific Invitation**

**1.1 General**

* + 1. The Government Procurement Administration, at the Division of the Accountant General, Ministry of Finance (hereinafter: **“the Administrator of the Tender”**) hereby promulgates a Specific Invitation to Tender for the supply of SSE (Secure Service Edge) products and related services therefor (hereinafter: **“the Specific** **Invitation”**). This Specific Invitation is being conducted as part of Central Tender 05-2022 for the procurement and supply of products and services in the field of information security and cyber defense for government ministries, support units, and associated entities (hereinafter: **“the Central Tender”**) and shall be marked as Specific Invitation no. 6.
    2. Only Framework Suppliers are entitled to participate in the Specific Invitation. In this document, a Framework Supplier shall also be termed a “Bidder.”
    3. **The Specific Invitation Documents shall not be distributed to any party other than one of the parties needed for the purpose of responding to this Invitation** and subject to said party undertaking to maintain the confidentiality of the Specific Invitation Documents.
    4. The response to this Specific Invitation shall be submitted by the date specified in Appendix A—General Details of the Specific Invitation**.**
    5. It is stated for clarity that this Specific Invitation Document is an inseparable part of the Tender Documents and all obligations and rights specified in both the Tender Documents and in this document shall apply to the Framework Supplier.
    6. The Specific Invitation shall be conducted using the Dynamic Online Specific Invitation method. If the method of the Specific Invitation is revised, the Administrator of the Tender shall serve the registered suppliers with notice of said revision within a reasonable time for the possible submission of monetary bids for the Specific Invitation.
    7. In this Specific Invitation, a **single Winner** (hereinafter: **“the Winner”**) shall be chosen and shall be entitled to supply the entire line of products and services included in this Specific Invitation.
    8. It is stated for clarity that an inviting party that promulgated a tender or contracted with any supplier for the procurement of products and services in the domain of the Tender before the Winner of the Tender is announced may continue the tender proceeding and the contract until these expire in accordance with their terms. Furthermore, an inviting party may enter into contract for the purchase of products and services in the domain of the Specific Invitation by means other than this Tender per authorization of the Exemption Committee as defined in the Mandatory Tenders Regulations, 5753-1993.
    9. It is stated for clarity that the Administrator of the Tender may update the Specific Invitation Document and its appendices, at her or his sole discretion, within a reasonable time before the bid submission deadline as specified in Appendix A—General Details of the Specific Invitation.In such an event, the Administrator of the Tender shall send updated Specific Invitation Documents. Insofar as the Administrator of the Tender promulgates an updated version of the Specific Invitation Documents, the Bidder must ensure that its response is submitted in accordance with the updated wording.
    10. **It is hereby emphasized that neither the Winning Supplier nor the Manufacturer whose products it sells shall publish the fact of this contract or any of its details,** and that the Administrator of the Tender reserves the right not to promulgate a public instruction (a Finance and Administration Code [TAKAM] announcement) on the topic of this Specific Invitation and may instead disseminate it in some other way.
    11. The contact person for this Specific Invitation is Daniel Ben-Hamo at [GPA\_cyber@mof.gov.il](mailto:GPA_cyber@mof.gov.il).
    12. In every inquiry concerning this Specific Invitation, the title line of the electronic-mail message must state the number of the Specific Invitation, the name of the Specific Invitation, and the subject of the inquiry (for example: Specific Invitation no. **6**—**SSE Service**—**clarification questions**”).
    13. In submitting its bid, the Framework Supplier affirms that its bid meets all requirements of the Tender and the Specific Invitation, including specifications, terms of use, delivery times, the Specific Invitation periods, and so on, and that it has read, understood, and accepted the requirements in the Specific Invitation Document and the Administrator of the Tender’s answer to the clarification questions.

**1.2 Clarification Questions and Remarks**

1.2.1 **Submission of clarification questions and remarks**

1.2.1.1 Clarification questions and remarks concerning this Specific Invitation shall be sent to the electronic-mail address specified in Section 1.1.11 above by the deadline for the submission of clarification questions and remarks as specified in Appendix A—General Details of the Specific Invitation.

1.2.1.2 Said questions shall be submitted solely in the Excel file attached to the notice from the Administrator of the Tender about the promulgation of the Specific Invitation (hereinafter: **“Notice of Promulgation of the Specific Invitation”**), marked as Appendix A1.

1.2.1.3 The Framework Supplier shall ensure by return electronic mail that the question file has reached its destination. Failure to respond to a clarification question shall not serve as a reason for failure to submit a bid by the deadline set forth.

1.2.1.4 Questions submitted after the deadline or presented orally, by telephone, or in a format other than that required shall not require a response from the Administrator of the Tender.

1.2.1.5 Questions submitted anonymously shall not be answered.

1.2.1.6 The Administrator of the Tender may allow additional rounds of clarification questions and remarks by notifying the Framework Suppliers.

1.2.1.7 A Bidder that wishes to make remarks or express complaints about the Specific Invitation or its terms shall do so within the framework of the clarification-questions stage. It is stated for emphasis that after the bid is submitted, the Bidder shall maintain silence and shall not take issue with the terms of the Specific Invitation.

1.2.2 **Response of the Administrator of the Tender to clarification questions and remarks**

1.2.2.1 Answers and clarifications shall be given in writing only. They shall be worded in the obligatory manner and shall be an inseparable part of the Specific Invitation Documents.

1.2.2.2 Answers and clarifications from the Administrator of the Tender shall be sent to the Framework Suppliers. It is the responsibility of the Framework Supplier to keep updated regarding answers from the Administrator of the Tender and of ongoing updates that the Administrator of the Tender shall promulgate regarding the Tender and the Specific Invitation.

1.2.2.3 The Administrator of the Tender may revise the Specific Invitation Documents in any way and may interpret or clarify the provisions of the Tender and the Specific Invitation irrespective of clarification questions.

1.2.2.4 The Administrator of the Tender is not obliged to the wording of a question submitted and, within this generality, may, when formulating a response to clarification questions, abridge or revise the wording of the question.

1.2.2.5 The questioner’s identity shall not be revealed in the response to a clarification question or at all, other than where required by law.

**1.3 Submission of bids**

1.3.1 **General**

1.3.1.1 The Bidder shall submit **one** bid for the products and services of **one Manufacturer**.

1.3.1.2 To eliminate any doubt, a Bidder must comply with all requirements specified in this document. The requirements set forth by the Administrator of the Tender shall not be revised. Any such revision may result in disqualification of the bid at the discretion of the Administrator of the Tender.

1.3.1.3 Only responses to Appendices B–F are mandatory. There is no need to sign the response on each page and no need to sign elsewhere in the response documents unless this requirement is noted specifically (as in Appendix B).

1.3.1.4 Submission shall be made to the digital tender box, as set forth in Section 0 below. [לטיפולכם]

1.3.1.5 **The following documents shall be placed in the digital tender box as part of the response**:

|  |  |
| --- | --- |
| **Title of document** | **Remarks** |
| Authorization of Bidder | Signed by the Bidder’s authorized signatory in the wording attached as Appendix B   * **shall be submitted in.pdf format.** |
| Professional and technical requirements | Full response to the questions specified in Appendix C   * **shall be submitted in Word format.** * **Any document that the Bidder wishes to submit shall be attached to the response and shall refer to the appropriate sections of the document.** * **Links shall not be checked.** |
| Price list | The Manufacturer’s official price list.   * **shall be submitted in.pdf format.** * **The official price list shall be a District of Columbia price list, duly signed, all of which as set forth in Section 3.7.1 of the Central Tender documents.** |
| Licensing specification | The Manufacturer’s full licensing specification for all products included on its official price list.   * **to be submitted in.pdf format.** |
| Reference model | In accordance with the provisions of Appendix D1, attached to the notice of promulgation of the Specific Invitation   * **to be submitted in Excel format.** * **with attention paid to the provisions of Sections 3.7.4 and 3.7.5 of the Central Tender Documents.** |
| Manufacturer’s affirmation | In accordance with the wording attached herewith as Appendix E.   * **to be submitted in.pdf format.** * **The affirmation may be submitted in Hebrew or in English.** |
| Request for confidentiality of details in the bid | In accordance with the wording attached herewith as Appendix F.   * **to be submitted in Word format.** |
| Posting of representative to the Merav system | In accordance with the wording attached as Appendix 1 of Booklet 2 of the Tender Documents.   * **to be submitted in.pdf format.** * **to be submitted only in the event that the Bidder wishes to change its representative.** |
| Additional documents | Appendices including certifications, brochures, and so onmay be attached to the response if necessary.   * **to be submitted in the format in which they were originally produced**. |

1.3.2 **Submission of bids in the Specific Invitation**

1.3.2.1 A Bidder that is interested in participating in the Specific Invitation shall place its response, as specified above, in the electronic tender box by means of the online bid submission system.

1.3.2.2 A link to the bid submission system shall be sent to the Framework Suppliers at least five working days before the bid submission deadline.

1.3.2.3 The deadline for the placement of bids in the digital tender box is specified in Appendix A below*.*

1.3.2.4 For the purpose of submitting its bid, the Bidder shall identify itself by means of the National Identification System and shall register in advance with the bid submission system.

1.3.2.5 After said identification is performed, it shall be ascertained that the details of the relevant Specific Invitation appear in the bid submission system.

1.3.2.6 In submitting its bid, the Bidder shall act in accordance with the instructions that shall appear in the bid submission system, shall fill in all requisite fields clearly and in accordance with the system’s instructions, and shall upload to the system the files required under the provisions of the Tender and the Specific Invitation.

1.3.2.7 After the submission of the bid in the system is completed, a reference number shall appear on the submission screen. In the event that no reference number is received, the bid has not been submitted. In addition, once the submission is completed, the system will send an electronic-mail message containing the data of the bid including all files submitted and the time of their submission, to the electronic-mail address that the user fed into the system. The details of the bid submitted to the system may be verified against the electronic-mail message or placed again into the box and the details of the bid may be confirmed against those appearing in the bid.

1.3.2.8 Bids may not be submitted to the system after the bid submission deadline.

1.3.2.9 **The Bidder may make one submission only!** After the bid submission is completed, no additional submission or update of the bid shall be allowed.

1.3.2.10 In the event of a technical malfunction that prevents the submission of bids in the Tender, the Administrator of the Tender may, by notifying the Framework Suppliers, establish an alternative way of bidding in the Tender.

1.3.2.11 Additional conditions for use of the bid submission system:

1.3.2.11.1 The maximum size of each file in the bid is 10 MB and the maximum size of all files together in the same bid is 50 MB. The Bidder shall check the size of the files that it sends and ensure that its bid complies with the limitations.

1.3.2.11.2 Files may be uploaded to the system in.pdf / Word / Excel format.

1.3.2.11.3 The number of characters in the name of a file that is uploaded is limited to a maximum of 64.

1.3.2.11.4 Technical assistance: For technical matters and assistance in operating the system, the support hotline may be contacted on Sunday–Thursday, 8:00–17:00, by using the following link: <https://merkava.mrp.gov.il/ccc/index.html>. In such an inquiry, the title of the Tender and the bid submission deadline shall be noted and, where necessary, screenshots shall be attached. The wait time from the moment the inquiry is sent until the response of a service representative shall not exceed four hours within the range of the hotline’s hours of activity. In exceptional cases only, wait time may exceed four hours. The support hotline is not obliged to respond to inquiries received within less than four hours from the bid submission deadline.

1.3.2.11.5 **After 20 minutes pass with no action taken, the system will disengage and any action carried out in it and not saved as a draft will not be saved.** In this case, reentry to the system shall be needed. To familiarize itself with the other limitations of the system, the Bidder shall read the bid submission manual [קישור] in advance. In addition, training materials that are meant to help the Bidder to submit its bid successfully are available to the Bidder (link: <https://portal.gpa.gov.il/supplier/tender>).

1.3.2.11.6 The instructions and training materials as to how to place bids in the electronic tender box may be accessed through the following link: [https://portal.gpa.gov.il/supplier/tender](https://portal.gpa.gov.il/supplier/tender/).

1.3.2.12 The Bidder is solely responsible for submitting the bid before the bid submission deadline. The Bidder shall bear in mind that as the bid submission deadline approaches, the bid submission system may be overloaded or may malfunction in other ways that may prevent the Bidder from submitting its bid. **The Bidder must prepare for this possibility and submit its bid in a timely manner.** The Bidder will not have any claim against the Administrator of the Tender in regard to a malfunction discovered in the bid submission system shortly before the bid submission deadline even if it was unable to submit its bid as a result.

**1.4 Bid review procedure**

1.4.1 Bids in the Specific Invitation shall be reviewed in accordance with the rules specified in the Central Tender Documents, with emphasis on “Booklet no. 2 of the Tender Documents: Instructions concerning Part B of the Tender” (hereinafter: **“Booklet no. 2 of the Tender Documents”**):

1.4.2 **Stage 1: Calculating the quality score**

1.4.2.1 A minimum quality score has been established for this Specific Invitation, as specified in Appendix A. Also specified in Appendix A are the weights for the issuance of the quality score as part of the Specific Invitation. Bids that receive a quality score below the minimum quality score established in Appendix A shall not progress to the dynamic phase of the Specific Invitation.

1.4.2.2 After all bids in the Specific Invitation receive quality scores, they will be weighted such that the bid with the highest quality score shall receive a weighted quality score of 100, whereas the other bids shall receive scores prorated to the ratio of the quality score of their bid to the bid that received the highest quality score, in accordance with the following formula:

Weighted quality score of the bid reviewed = the quality score of the bid reviewed divided by (÷) the quality score of the bid that received the highest quality score among all bids in the Specific Invitation, multiplied by 100. For example, if the highest quality score is 90 and the score of the bid reviewed is 72, the weighted quality score of the bid examined will be  = 80 points.

1.4.3 **Stage 2—Calculating the weighted price**

1.4.3.1 Bidders with bids satisfying the minimum terms and exceeding the minimum quality score, as the case may be, will be invited to participate in the online dynamic stage of Specific Invitation, on the date specified in Appendix A.

1.4.3.2 The online dynamic stage shall be conducted in a new Specific Invitation system—the Merav system (hereinafter: **“Merav System”**) in a British specific invitation model. (For an explanation of this model, see Appendix 2 of Pamphlet 2 of the Central Tender Documents.) The Administrator of the Tender shall hold a training session for interested Bidders about the Merav system before the Online Dynamic Specific Invitation is held.

1.4.3.3 Notice of the date of the training session for the Merav system shall be sent to all Framework Suppliers by electronic mail.

1.4.3.4 The registration method and the emphases in using the Merav system are specified in Appendix G.

1.4.3.5 In the Online Dynamic Specific Invitation, the Bidder shall enter the following:

1.4.3.5.1 The percent discount off the official list price for all products offered by the Bidder in the Specific Invitation.

1.4.3.5.2 Maintenance service costs as specified in the relevant sections of Appendix D (maintenance costs, cost per work hour, and so on), all of which in accordance with the details in the Appendix.

1.4.3.6 These components shall be weighted in the course of the Specific Invitation as set forth in the Reference Model (Appendices D, D1).

1.4.3.7 The weighted price of the bid in the Online Dynamic Specific Invitation shall in no case exceed the maximum price in the bid as set in accordance with the provisions of Section 1.4.5.4 below*.*

1.4.3.8 In the event that the weighted price of the bid exceeds the maximum price established in the bid, the Administrator of the Tender shall suspend the Specific Invitation, serve the Bidder with warning to this effect, and allow it to tender an additional bid. If said Bidder fails to tender a bid as aforesaid, the Administrator of the Tender shall terminate the Bidder’s participation in the Specific Invitation and shall view this as a breach of the Bidder’s undertakings.

1.4.3.9 The final price of all relevant products of the Manufacturer shall be the official list price less the discount rate that the Bidder offers for the products. It is stated for clarity that the Winning Bidder may offer an improved price at the end of the Specific Invitation.

1.4.3.10 In the event that the Bidder wins two or more Specific Invitations and some items are shared by both Specific Invitations or more, the price shall be the lowest price set among the prices offered for the product.

1.4.3.11 Framework Suppliers that are interested in additional training in the use of the Online Dynamic Specific Invitation system (beyond the predetermined training sessions to which they were invited) shall give notice of their wish to do so together with their documents of response to the application for the Specific Invitation.

1.4.4 **Stage 3—Setting the price score**

1.4.4.1 The price score shall be derived from the weighted price of the bid, using the following formula:

1.4.4.2 Definitions:

*TPi*—price score of Bidder *i*

—weighted price of Bidder *i*

*Lowest price received—*the lowest weighted price received from any of the Bidders

*Median price—*the median price among all prices submitted by Bidders that satisfied the requirements in Section 1.4.3.1 above in response to the Reference Model. (In the event of an even number of bids, the average of the two middle bids shall be calculated.)

1.4.5 **Stage 4—Calculating the bid score and ranking the bids**

1.4.5.1 The price score shall be weighted together with the weighted quality score of the bid in accordance with the contents of Section 1.4.5.2 below and shall constitute the bid score. The bids shall be ranked in accordance with the bid scores that they received, the highest-scoring bid ranking first. The bid score shall be determined by the use of the following formula:

1.4.5.2 Definitions:

*Gi*—the bid score of Bidder *i*

*Qi—*the weighted quality score of Bidder *i*

*TPi*—the price score of Bidder *i*

*Wq*—quality weight

*Wp—*price weight

1.4.5.3 Below are the weights in this Specific Invitation:

|  |  |
| --- | --- |
| **Component** | **Weight** |
| Weight of quality (*Wq*) | 60% |
| Weight of price (*Wp*) | 40% |

1.4.5.4 **Maximum price**

1.4.5.4.1 Before conducting the Online Dynamic Specific Invitation, the Administrator of the Tender may set a maximum bid price. In this case, one maximum price shall be set for all Bidders.

1.4.5.4.2 The maximum price shall be presented to the Bidders at least seven working days before the date of the Online Dynamic Specific Invitation.

1.4.5.4.3 After receiving the maximum price, the Bidder may withdraw its bid in the Specific Invitation without this being considered failure to comply with the terms of the Tender. Said withdrawal of bid shall be carried out in writing within two working days of the date on which the maximum price is sent to the Bidder. A Bidder that does not withdraw its bid as aforesaid assents to said maximum price and to its continued participation in the Specific Invitation proceeding.

1.4.5.5 **Simulated Specific Invitation**

1.4.5.5.1 A simulated Specific Invitation shall be held in the manner spelled out in Section 2.9.4 of Appendix 2 of Booklet 2 of the Central Tender Documents.

1.4.5.5.2 The simulated Specific Invitation shall take place on the date specified in Appendix A.

1.4.5.5.3 Participation in the simulated Specific Invitation is mandatory and is a condition for the Bidder’s participation in the Online Dynamic Specific Invitation.

1.4.5.5.4 If the Administrator of the Tender decides to revise a given detail in the rules of the Specific Invitation and if said revision, in his or her opinion, has the effect of changing the conduct of the Specific Invitation significantly, he or she may announce the performance of an additional simulated Specific Invitation. In such a case, the rules set forth above shall apply with the required changes.

1.4.6 **Sole bid**

1.4.6.1 Without derogating from the contents of Section 1.5.2 of the Central Tender Documents, if only one bid is submitted in the Specific Invitation or only one bid remains after the bids are reviewed, the Administrator of the Tender may, at his or her sole discretion:

1.4.6.1.1 declare the remaining Bidder the Winner;

1.4.6.1.2 cancel the Specific Invitation and launch a new Specific Invitation.

**1.5 Details of the contract**

1.5.1 The rules specified in Chapter 3 of the Central Tender Documents—Method of Performing and Implementing the Contract—shall apply to the contract emanating from this Specific Invitation. Conditions specific to this Specific Invitation are spelled out below.

1.5.2 **Term of the Contract**

1.5.2.1 The Term of the Contract emanating from this Specific Invitation (hereinafter: **“the Term of the Contract in the Specific Invitation”**) shall be 36 months from the date on which the Administrator of the Tender apprises the Winner of the Specific Invitation of the onset of the Term of the Contract. The Administrator of the Tender shall have the option of extending the contract in additional periods of up to 36 months (total: 72 months) by serving prior notice at least fifteen days before the end of each Term. Throughout the Term of the Contract of the Specific Invitation, Customers may buy the products and services from the Winning Supplier.

1.5.2.2 The first 21 working days of the Term of the Contract in the Specific Invitation shall be defined as a getting organized period. During this time, the Winning Bidder shall complete its preparations for delivery of the sought-after products and services.

1.5.3 **Warranty and maintenance**

1.5.3.1 Without derogating from the contents of Section 3.13.1 of the Central Tender Documents, the first warranty, service, and maintenance period, or the subscription period, of the procured products and services (including expansions, licensing, subscription fees for a particular service, and software included in the sale of the goods) shall be included in the price of the product or the service and shall be valid for 12 months from the date of **product** **activation** and, insofar as the Customer purchases installation and assimilation services, from the date of the Customer’s confirmation that the Supplier has carried out said installation to its satisfaction and as required, whichever is later (hereinafter: **“the First Warranty Period”**). In a case where, in the opinion of the Administrator of the Tender, a delay has occurred in obtaining the Customer’s confirmation for reasons beyond the Supplier’s control, the Warranty Period shall begin on the day the Supplier completes all of its performable undertakings as the Administrator of the Tender shall determine.

1.5.3.2 The winning Bidder shall provide additional warranty and maintenance periods beyond the First Warranty Period, up to 72 months from the end of the Term of the Contract of the Specific Invitation (**“the Warranty and Maintenance Period”**), that is, mandatory warranty and maintenance may continue even after the Term of the Contract ends.

1.5.3.3 It is stated for clarity that if a subscription sale model is used, the warranty and maintenance services shall be provided at the subscription price throughout the subscription period (even if said period does not coincide with the Term of the Contract) as long as the Customer pays for the subscription and no further cost is required for warranty and maintenance even in the case of renewal of the subscription.

1.5.3.4 **Expansion of services to 24/7 service**

1.5.3.4.1 A Customer may choose whether to receive warranty and maintenance services within a 24/7 call window at with the level of service specified in Section 3.13.6.3.5 of the Central Tender Documents.

1.5.3.4.2 To expand the level of service, the Supplier will be paid additional recompense in accordance with the following:

1.5.3.4.2.1 For a product or service purchased—recompense at the rate of 15% of the annual maintenance price offered in its bid. For example, for a product that costs $5,000, with an annual warranty and maintenance cost amounting to 10% of the purchase price, the Supplier shall be recompensed in the sum of $75 for each year in the First Warranty Period and a total recompense of $575 for each additional year of warranty and maintenance. (The annual maintenance cost for each of the additional years is 10% x 5,000=$500; the added recompense for the expansion of services is 15% x 500=$75.)

1.5.3.4.2.2 For a product or service under subscription—recompense at the rate of 5.25% of the annual subscription cost. For example, for a product that costs $1,500 per year, the Supplier shall be paid $78.75 for each year in which the service is needed (5.25 % x 1,500=$78.75).

1.5.3.4.3 It is stated for clarity that a Customer may activate and deactivate the expansion of services at any time, said deactivation of services going into effect one full calendar year from activation.

1.5.4 **Licensing**

1.5.4.1 Whenever an organizational change occurs (including splitting or merger of offices or units), the Customer may convert any licensing into parallel licensing with the same Customer or may transfer licensing to another Customer by apprising the Supplier of said change.

1.5.4.2 Licensing for the purpose of establishing a review laboratory [a testing laboratory?—NG] shall take place at no cost and shall be limited to 30 days.

1.5.4.3 The Manufacturer shall maintain a license management interface that all Customers may access by means of the Internet, in which the Customer, after identifying itself, may receive a report on all licenses recorded in its organization, their validity, the validity of the maintenance agreement, and so on. The Customer may ask that its identity not appear in the system and the Supplier shall refrain from uploading it to the system if said request is given in advance, or shall delete it from the system as required within five working days. Alternatively, and with the Customer’s consent, the Customer’s ID may be revised to another ID that is determined in coordination with the Customer.

1.5.4.4 The licensing cost for establishing a passive DR or an “active-standby” system shall be 20% of licensing cost as determined in the Specific Invitation.

1.5.5 **Installation and assimilation of procured products and services**

1.5.5.1 The Customer may also procure installation and assimilation services as part of the sought-after products and services, doing so in accordance with the provisions of Section 3.8.4 of the Central Tender Documents and the provisions of Appendix D.

1.5.5.2 If the Customer procures installation and assimilation services, the Supplier, in coordination with the Customer, shall prepare to set up the project and perform the requisite works, and for this purpose shall coordinate with the Customer the contents of the work in accordance with the provisions of Sections 3.9.6–3.9.8 of the Central Tender Documents and in accordance with the provisions herein below.

1.5.5.3 As the products and services are being installed and assimilated, insofar as the Customer orders said services, the Supplier shall determine all requisite definitions in accordance with the contents of the Tender Documents, the Customer’s guidelines, and the producer’s best practices, up to full and sound operation of the project.

1.5.5.4 In addition, the Supplier will instruct the Customer’s personnel in the full and independent operation of the system so that after the installation and assimilation proceeding is completed, the professional teams of the Supplier shall have the requisite knowledge to operate the product routinely, fully, and independently.

1.5.6 **Recompense for installing and assimilating procured products and services**

1.5.6.1 For each hour of installation and assimilation actually carried out (hereinafter: **“hour worked”**), the Supplier shall be recompensed in the sum of NIS 250 (including Value Added Tax) per hour worked.

1.5.6.2 Recompense for an hour worked outside accepted working hours shall be paid under the provisions of Section 3.8.4.4 of the Central Tender Documents.

1.5.6.3 The rate per hour worked shall be updated once every 12 months at the most, commensurate with the percent change that shall apply in the rate of the holder of the post known as “Expertise Level B Cyber Defense Application Person,” as indicated in the “maximum rates” table in the Finance and Administration Code (TAKAM) notice that accompanies Tender 01-2009 for the Provision of Computer Services to Government Offices (as of the date on which the Specific Invitation was promulgated, the notice number was 16.2.11 for “Provision of Computer Services for Government Offices”—<https://takam.mof.gov.il/document/HM.16.2.11>) or any notice that shall replace it (hereinafter: **“Computer Services Tender”**).

1.5.6.4 Insofar as the rates in the Computer Services Tender are updated, the Supplier shall ask the Administrator of the Tender to update the rate per hour worked. As of the date on which the Specific Invitation was promulgated, the relevant rate in the notice was NIS 204 (not including Value Added Tax) per hour.

1.5.6.4.1 The following is an example of the way this indexation is carried out: If the rate for an “Expertise Level B Cyber Defense Application Person” is raised to NIS 220 during the Term of the Contract, that is, a 7.84% increase, the Supplier may, 12 months after the beginning of the contract or from the date of the previous change in the rate (whichever is later), request an increase in the rate per hour to NIS 269.60 (including Value Added Tax). This update shall apply to price quotes that shall be offered from the day on which the rate adjustment is approved and shall not apply to quotes presented to Customers or to orders filled.

1.5.6.5 If the Computer Services Tender is revised or if another central contract is executed in the matter such that the job definition of the “Cyber Defense Application Person” is eliminated or revised, or if the levels of expertise are eliminated/revised, the Administrator of the Tender may, at his or her sole discretion, choose some other type of post and level of expertise in order to activate the update mechanism.

1.5.7 **Team of service providers**

1.5.7.1 In addition to the provisions of Section 3.6.2.2.2 of the Central Tender Documents, a Customer may instruct the Winner to replace an application person at any time and for any reasonable cause, and the Winner shall appoint another application person in his or her place for the Customer within 21 working days.

1.5.8 **Addition of products and services to the list of products approved for procurement**

1.5.8.1 The list of products approved for procurement in the domain of the Specific Invitation shall be determined by the Administrator of the Tender in consultation with the winning candidate before the Term of the Contract in the Specific Invitation begins. During the Term of the Contract and in accordance with the Customers’ needs, the Administrator of the Tender shall update the list of products approved for procurement in the domain of the Specific Invitation. The discount rates that were established in the Specific Invitation shall apply to the list of approved items in the domain of the Specific Invitation. If a manufacturer of products or a supplier of services in the domain of the Specific Invitation has such that are suitable for on-premises installation, the Administrator of the Tender may add them to the list of products approved for procurement as specified above. However, the discount rates established in the Specific Invitation shall not apply to said items; instead, they will be negotiated and, in any case, shall not be less than the discount rate established in the Specific Invitation.

1.5.8.2 In addition to the foregoing, the Administrator of the Tender reserves the right, after the Specific Invitation and during the entire procurement period, to add to the contents of the contract products and services that are outside the domain of the Specific Invitation and that are needed for the efficient and maximal use of the items in the domain of the Specific Invitation, among the following categories including:

1.5.8.3 Installation, maintenance, service, and additional training.

1.5.8.4 Interfacing applications and software.

1.5.8.5 Hardware for structured test running of services in the domain of the Specific Invitation.

1.5.8.6 The price of the added item shall be determined in negotiations between the Administrator of the Tender and the Winning Supplier, with attention to the price of the item or service in Israel or abroad, the Manufacturer’s price list, and other manufacturers’ price lists, weighting the terms of services relevant to the Tender and the nature and use of the item.

1.5.8.7 The extent of procurement of items added during the Term of the Contract shall not exceed, cumulatively, 20 percent of procurements conducted through the Specific Invitation.

1.5.9 **Information processing and security and cyber defense in services**

1.5.9.1 In addition to the provisions of the Tender Documents and Appendix C of the Specific Invitation Document, rules pertaining to the manner of service delivery are specified in Appendix H.

1.5.9.2 These rules shall oblige the Supplier and the Manufacturer that the Supplier proposes for delivery of service within the framework of the Specific Invitation.

1.5.10 **Performance guarantee**

1.5.10.1 In accordance with Section 11 of the contract agreement and Section 2.12.3 of Booklet no. 2 of the Central Tender Documents, the winning candidate shall post a performance guarantee in the sum of NIS 500,000. Said guarantee shall be a digital guarantee in accordance with Section 11.3.2 of the Central Tender Documents.

1.5.10.2 Said guarantee shall be in effect for 90 days from the end of the Procurement Period or the last Warranty and Maintenance Period, whichever is later.

**2. Appendix A—General Details of the Specific Invitation**

**2.1 Specific Invitation dates**

|  |  |
| --- | --- |
| **Stage of the Specific Invitation** | **Date** |
| Deadline for submission of clarification questions and remarks | November 20, 2023 |
| Administrator of the Specific Invitation answers clarification questions | At least 12 days before the bid submission deadline |
| Opening of digital tender box for submission of bids | December 18, 2023, at 9:00 |
| Deadline for submission of bids | December 25, 2023, at 13:00 |
| Bid remains in effect until | June 25, 2024 |
| Simulated Specific Invitation (for bids that satisfy the requirements of the Specific Invitation) | To be sent separately |
| Online Dynamic Specific Invitation (for bids that satisfy the requirements of the Specific Invitation) | To be sent separately |

2.1.1 These dates are provided for informational purposes only and do not constitute certification of the soundness of the bid and participation in the Online Dynamic Specific Invitation.

2.1.2 A Bidder may participate in the Online Dynamic Specific Invitation only if the Tenders Committee certifies its bid for participation in the Specific Invitation.

2.1.3 Bids shall remain valid until the date shown above. The Administrator of the Tender may announce an extension of the validity of bids for an additional 90-day period (and, with the consent of the Framework Supplier, beyond this) until a Winner is chosen. The Bidder may not retract its bid during said period.

**2.2 Minimum quality score and scoring weights**

2.2.1 The minimum quality score for this Specific Invitation in the transition to the Online Dynamic Specific Invitation stage is **80%** (after the component of “assessment of scale and capability of development center in Israel” is neutralized). Similarly, the minimum quality score set for the weight of “assessment of method of cloud implementation, cyber defense, information security, and confidentiality in the proposed solution” is 85%.

2.2.2 The weights used to calculate the quality score are specified below:

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Topic** | **Weight** | **Minimum quality score** |
| 1. | Assessment of the product line offered (scale of the proposed system, system capabilities, system configuration, support of different cloud infrastructures, performance, compliance with open standards, system flexibility and adaptability to different operating structures, scale of management system, capabilities of integration and adaptability to existing and tangential systems, assessment of needs and rapidity of assimilation, additional capabilities beyond those required, scope of product line, and so on). | 40% |  |
| 2. | Assessment of method of cloud implementation, cyber defense, information security, and privacy offered by the proposed solution (how the cloud solution is implemented, business continuity and SLA, protection and security of processes and infrastructures, protection of customers’ information, and so on). | 15% | 85% |
| 3. | Assessment of Manufacturer (status in the market), assessment of its research entities, reporting and transparency policies, proven experience, support array, authorizations and compliance with Israeli and international standards, breadth of Manufacturer’s security solutions and interfaces with tangential products, and so on). | 10% |  |
| 4. | Assessment of scale and capability of development center in Israel. (If the Manufacturer has undertaken to establish such a center if it wins the Tender, partial scoring will be given.) | 15% |  |
| 5. | Assessment of Bidder’s ability (experience in the field and in similar fields, no. of employees in the field, relevant training activities, and so on). | 20% |  |
| **Total** | | 100% | **80%** (Excluding the “assessment of scale and capability of development center in Israel” component) |

**3. Appendix B—Bidder’s Certification**

We, authorized signatories for \_\_\_\_\_ (Bidder’s name), certify by affixing our signatures that:

1. We have read the Specific Invitation Documents, including their Appendices.
2. We understand and accept every section of the Specific Invitation Documents and shall be enjoined and silenced against bringing any claim against the terms of the Specific Invitation from the moment the bid for the Specific Invitation is made.
3. The details appearing in this Bid, including its Appendices, are true and the Bidder is able, and intends, to comply with every detail in its Bid and with the instructions of the Tender and the Specific Invitation.
4. This Bid, including all its details, was prepared independently by the Bidder, without consultation, arrangement, or connection with any other Bidder.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date | Full name | Position in the Bidder’s organization | Signature and stamp |

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Date | Full name | Position in the Bidder’s organization | Signature and stamp |

**(This document may be signed electronically, provided it be ensured that said signature was affixed by the relevant signatory and that the file was not modified after signature.)**

**4. Appendix C—Technical Requirements**

**4.1 Guidelines for responding to this Appendix**

4.1.1 Sections in which there is a requirement for detail only **are not mandatory requirements** and the Bidder shall give a clear detailed account of the Manufacturer’s capabilities or the proposed solution, if these capabilities are supported in the Bidder’s response. It is stated for clarity that failure to provide an answer in a Section of this kind shall be construed as lack of support for the proposed solution in the capabilities spelled out in this Section.

4.1.1.1 If these Sections are nonexistent in the proposed solution by the bid submission deadline but are expected to become existent, the schedule shall be noted.

4.1.2 Sections in which an explicit demand for a characteristic or capability is expressed are **mandatory sections** and no bid shall be accepted that does not include a response to the demand or the capability specified in the Section. Insofar as details are required in said Section as to the manner of the response, the Bidder shall provide said details as required.

4.1.2.1 Unless stated otherwise in the specific Section, the proposed system shall comply with all mandatory sections in this Appendix **by** **the bid submission deadline in the Specific Invitation.**

4.1.3 **It is stated for clarity that all Sections in Appendix C shall be included in bid assessment and scoring.** For each characteristic or capability supported, a detailed response is required as to whether said ability or characteristic is included among the items proposed in the Reference Model or whether their actualization requires additional procurement or licensing.

4.1.4 **It bears emphasis that failure to reply, replying in a way that fails to satisfy the requirement, failure to respond to the requirement, or replying vaguely or ambiguously may result in low scoring or disqualification of the Bid at the sole discretion of the Administrator of the Tender.**

4.1.5 A response to this Appendix may be submitted in Hebrew or in English.

**4.2 Terms and requirements for Manufacturer and Bidder**

4.2.1 In addition to maintaining an active service hotline by the Bidder as specified in Section 3.13.6.2 of the Central Tender Documents, **the Manufacturer** shall provide a support center that will serve as an address for professional inquiries and questions (hereinafter: **“the Support Center”**), through which a response may be obtained within 24 hours in one or more of the following ways: **(a)** telephone response, active in ordinary working hours as these are defined in Section 3.10.1 of the Central Tender Documents; **(b)** a portal for opening service requests; (c) a dedicated electronic mail address for the purpose of this Tender. The Bidder shall provide details of the Manufacturer’s service covenant (SLA), method of making contact, address/telephone number, and how the hotline shall operate. The Administrator of the Tender may set rules regarding how the Support Center may be contacted.

4.2.2 The Support Center shall provide support in English. A detailed account regarding the ability to offer support in Hebrew is required.

4.2.3 The Winner shall provide Manufacturer with recommendation (Best Practices) documents for the recommended configuring and protections that it provides for the SSE field on the basis of accepted methodologies, including reference to the manner of product use in order to comply with an accepted security standard such as ISO-27002 and NIST.

4.2.4 The Bidder shall explain in detail the Manufacturer’s policies regarding the Manufacturer’s transparency and reporting of security problems/exposures discovered in its products in the domain of the Specific Invitation, or in relation to any breach or other information exposure in its products, including the amount of time needed to report them.

4.2.5 **Location of product development**

4.2.5.1 The Bidder shall specify the location where the products in the domain of the Specific Invitation are developed and shall attach a Manufacturer’s certification accordingly.

4.2.5.2 If the Manufacturer undertakes to establish a development center in Israel in the domain of the Specific Invitation, details about this shall be provided and the Manufacturer’s commitment in accordance therewith shall be attached.

4.2.6 **Details concerning the Bidder’s experience with the product offered**

4.2.6.1 A detailed account is required of the Bidder’s experience with the product offered, including the year in which it began working with the proposed Manufacturer, the level of Manufacturer’s certification of the Bidder for the system offered, and all other relevant information.

4.2.6.2 A detailed account is required of all application personnel whom the Bidder employs and who are certified by the Manufacturer for the products and services offered in the Specific Invitation, in the following format:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Employee’s name** | **Years of experience with the product** | **Certification for the proposed products** | **Year of certification** | **Security clearance, if any** |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |

4.2.7 The Bidder has an active service hotline as specified in Section 3.13.6.2 of the Central Tender Documents.

4.2.8 The Bidder shall give a detailed account of the way it supports the following services:

4.2.8.1 consulting and assistance in defining the proposed solution offered to Customers—the nature of the proposed services shall be explained in detail.

4.2.8.2 assistance on the Customer’s site—the processes of assistance and escalation shall be specified in detail.

4.2.8.3 professional training for Customer’s employees, including formal training and certification by manufacturer-certified elements—a detailed account is required regarding the types of courses and certifications given both by the Bidder and by the Manufacturer.

**4.3 System/product requirements**

4.3.1 The **Secure Service Edge (SSE)** services, for the purpose of this Specific Invitation, are the totality of tools and technologies (including **SWG, ZTNA, and CASB**) that serve as a platform for the mitigation of risks of information loss and denial of unauthorized access to local, cloud-based, and online resources, and for the mitigation of information degradation incidents.

4.3.1.1 For this purpose, it is stated for clarity that endpoints may be workstations, mobile computers, a server, a cloud component, a mobile device, and so on.

4.3.2 The systems and licenses offered in the Reference Model shall include all requirements specified in this Appendix, at no additional cost, including interfacing capabilities for third-party products that the Specific Invitation Documents mandate.

4.3.3 The Bidder’s price quote shall include all requisite components for response to the requirements of the Central Tender Documents and the Specific Invitation, the specifications, and the Reference Model. The Bidder, in its bid in the Specific Invitation, undertakes that all products and services that it offers in the Specific Invitation are available in ongoing manufacture and that neither it nor the Manufacturer has any information or concern about the end of sale, production, delivery, or support of the products and services (or components and items that they use) that it offers.

4.3.4 It shall be ensured that the price quote for each of the components needed for the Reference Model (Section 4.3.7) includes all requisite licensing for system operation and use.

4.3.5 A clear and comprehensible licensing specification for each proposed component in accordance with the Reference Model shall be attached and the licensing model (perpetual, subscription, and so on) shall be noted.

4.3.6 A Manufacturer’s Best Practices document relating to license management, optimization, and operation shall be attached.

4.3.7 **An itemization of the requisite products follows**:

4.3.7.1 **Cloud software SSE product services (SaaS)**:

|  |  |  |
| --- | --- | --- |
| **Topic** | **Proposed response** | **Remarks** |
| SSE licensing and support for 50,000 licenses |  | Give a detailed explanation of all product supplied in the Bidder’s bid, including management system and system-survivability components.  This number is the estimated number for all Customers  Your attention is called to Section 5.5.1 of Appendix D below. |
| A management system that supports 50,000 licenses, including survivability and support for multi-tenant management. |  |
| A detailed account is required regarding the hardware needed for installation of the management system (including survivability). |  |

**4.4 Technological requirements**

4.4.1 **Configuration requirements**

4.4.1.1 Support in two configurations —private government cloud and public government cloud—is required. A detailed account is required regarding the deployment of both configurations from hardware and software standpoints.

4.4.1.2 Support of the undegraded survivability of end-user activity is required. A detailed account is required regarding the way this requirement shall be fulfilled.

4.4.1.3 Support of system assimilation on the DR site shall be provided.

4.4.1.4 The system shall support assimilability on the following platforms:

4.4.1.4.1 Microsoft SQL DB.

4.4.1.4.2 Standard.

4.4.1.4.3 Enterprise.

4.1.1.4.4 Windows Server 2016 and up.

If there are additional platforms on which the system may be assimilated, make note of this.

4.4.1.5 Details on whether there is a need to assimilate additional components into the Image configuration, such as OVA (Linux), shall be given.

4.4.2 **Central architecture for operation and application of management and enforcement policy**

4.4.2.1 The system must support multi-tenant management with specific authorizations for the license-management system and for ministries of different sizes, with a private and public government cloud solution.

4.4.2.2 Assimilability into high-availability architecture is required.

4.4.2.3 Central management ability from a console is required.

4.4.3 **Secured access to Web and Cloud infrastructures**

4.4.3.1 System deployment

4.4.3.1.1 The Bidder shall offer a local/Israeli support base for the product offered and for its deployment, as specified in the Tender Documents and the Specific Invitation.

4.4.3.1.2 Support of the following capabilities under integral central interface management is required:

4.4.3.1.1.1 Proxy (Security Improvement topology, Cache & Authentication.

4.4.3.1.1.2 Anti-Malware.

4.4.3.1.1.3 URL Filtering.

4.4.3.1.1.4 SSL Termination/Inspection.

4.4.3.1.1.5 Protocol Filtering (Application Filtering).

4.4.3.1.1.6 Reporting.

4.4.3.1.2.7 Quota enforcement.

4.4.3.1.2.8 CASB Integration.

4.4.3.1.2.9 CDR Integration.

4.4.3.2 The product shall support IPV6, NTP, and DNS traffic.

4.4.3.3 System support in High Availability (NA) configuration and communication and power-supply redundancy are needed. A detailed account is needed in regard to how the system will comply with this requirement.

4.4.3.4 Mechanism support that allows immediate blockage of all communication to the internet, for use in the event of a malicious breach and/or attempted breach (e.g., a panic button), shall be required.

4.4.3.5 The solution shall support work with several segments and traffic monitoring from several segments such as DMZ, WAN, and Wi-Fi.

4.4.3.6 The management array shall allow integrated access with strong MFA ID mechanisms.

4.4.3.7 Integration atop the program that includes the organization’s existing information-security controls, such as DLP, CASB, and others, shall be provided.

4.4.3.8 The product shall allow secure search on the basis of the system’s engines (application blocking, URL categorization, etc.).

4.4.3.9 The solution shall allow for a code of conduct [constitution במקור: "חוקה":] based on geolocation or hours of activity to be built.

4.4.3.10 The reporting mechanism on code-of-conduct [חוקה] breach shall include the following parameters among others:

4.4.3.10.1 user name.

4.4.3.10.2 IP address.

4.4.3.10.3 the rule breached.

4.4.3.11 Policy toward users outside the organization and users in the organization’s offices shall be managed from a central management platform.

4.4.3.12 The solution shall make it possible to limit users’ downloading to a certain quantity of specified data, for example, downloading no more than 1 GB during a fixed period of time.

4.4.3.13 The solution shall make it possible to set a specific time for backup of system definitions. A detailed account shall be provided in regard to the backup method and additional requirements.

4.4.3.14 The solution shall support a Web-based central user management and interface architecture that includes monitoring, reporting, maintenance, and code-of-conduct and policy operation capabilities.

4.4.3.15 The management interface system shall be enabled by encrypted access protocols based on up-to-date protocols such as HTTPS and SSH.

4.4.3.16 The solution shall support RBAC-based management. A detailed account is required regarding default system-access profiles and of adaptability and construction of new profiles.

4.4.3.17 The solution shall support capabilities of blacklisting or whitelisting of objects such as user, IP address, URL addresses, and domains.

4.4.3.18 The system shall be able to block users from downloading various types of files on the basis of extensions.

4.4.3.19 The system shall be able to filter and obstruct predefined categories such as social networks and to apply intra-application limits such as blocking chat or video capability within a social network such as Facebook.

4.4.3.20 The solution shall include possibilities of user/group authentication for the following configurations at the very least:

4.4.3.20.1 Windows Authentication (Kerberos).

4.4.3.20.2 NTLM v1 and v2 in Session Security.

4.4.3.20.3 LDAP.

4.4.3.21 A detailed account is required regarding the ability of the solution to support the XFF (X-Forward For) parameter for original customer address ID.

4.4.3.22 The solution shall allow dispatch of alerts to specific users by electronic mail and text message. A detailed account regarding additional possible ways of sending alerts is required.

4.4.3.23 The system shall allow real-time updates of threats and updates of signatures and addresses of malicious sites, porno sites, terror sites, religion-based sites, gambling sites, attack sites, proxy and anonymization sites, malicious software commands, C&C sites, bot networks, ransomware ID databases, and other frauds.

4.4.3.24 A detailed account is required regarding the ability to time DB system-engine updates and the nature of said updates.

4.4.3.25 Support of SNMPv2c, V3 and up shall is required.

4.4.3.26 The solution shall support binding on the basis of:

4.4.3.26.1 user.

4.4.3.26.2 IP.

4.4.3.26.3 MAC.

4.4.3.27 Support of session time-out and idle time-out for enforcement of user disconnect is required.

4.4.3.28 Support of FTP Over HTTP protocol scanning is required.

4.4.3.29 The system shall offer the possibility of blocking pages that contain:

4.4.3.29.1 malicious JavaScript / VB Script.

4.4.3.29.2 malicious (or unauthorized) ActiveX applications.

4.4.3.29.3 potentially unwanted programs (PUPs);

4.4.3.29.4 malicious Windows executables.

4.4.3.30 The solution shall support scanning of various kinds of nested compressed files.

4.4.3.31 The solution shall offer the possibility of caching capabilities. A detailed account is required regarding cache capabilities, volumes offered, and latency.

4.4.3.32 The product shall allow the use of the Web Proxy auto-discovery protocol in order to enable system managers to establish a policy and dynamic proxy for users (auto-proxy configuration in the browser).

4.4.3.33 The product shall allow monitoring and blockage of immediate-message software and file transfer across the range of these software products.

4.4.3.34 The solution shall support DR configuration in the event of failure. A detailed account is required regarding the way the DR shall be implemented and technological requirements for this purpose.

4.4.3.35 The solution shall allow license expansion with no need for downtime.

4.4.4 **SSL**

4.4.4.1 The solution shall scan SSL and https traffic and provide decryption of traffic encryption and re-encryption capability.

4.4.4.2 A detailed account is required regarding the system’s ability to import a ServerSide Certificate and private keys for decryption encryption.

4.4.4.3 The solution shall support the SSLv3, TLS 1.2, TLS 1.1, TLD 1.0, and SSLv2 encryption protocols.

4.4.4.4 Support is required of the following algorithms: ECDHE, DHE, and RSA, as well as SHA, SHA-1, MD5, and 256 hash.

4.4.4.5 A detailed account regarding support of additional methods, such as Camellia, RC4, DES, 3DES, and AES, is required.

4.4.4.6 A detailed account regarding support of X.509 certificates is required.

4.4.4.7 A detailed account is required regarding support of the organization’s existing CA and its existing PKI mechanism, including performance of operations such as revocation management.

4.4.4.8 A detailed account regarding support of an HSM array is required.

4.4.4.9 Support of the OCSP stapling protocol is required.

4.4.5 **System engines**

4.4.5.1 Structural support of the ability to identify and block malware, centrally managed via the system interface, is required.

4.4.5.2 Support of Web isolation capability from a central management interface, with no need to operate across separate products, is required.

4.4.5.3 The solution shall provide court-admissible evidence when identifying malware on a network, including *inter alia*:

4.4.5.3.1 event timestamp.

4.4.5.3.2 network incidents in sequence.

4.4.5.3.3 packet capture of suspicious communication.

4.4.5.3.4 malware behaviors.

4.4.5.3.5 malware type.

4.4.5.3.6 severity.

4.4.5.3.7 source and target of attack.

4.4.5.4 Support of a malware detection solution composed of several engines and including, *inter alia,* signature- and heuristics-based detection capabilities is needed.

4.4.5.5 Support of detection of file-embedded malware, such as in .pdf files, is also needed.

4.4.5.6 Support of establishing a security policy based on different protocols, including definition of action confirmation ability, action blocking, monitoring, specifying use times, and defining authorized volumes is needed.

4.4.5.7 Ability to detect incidents on the basis of the following categories, at the very least, is required:

4.4.5.5.1 advanced malware command-and-control category.

4.4.5.5.2 advanced malware payload-detection category.

4.4.5.5.3 malicious embedded links and iframe detection category; mobile malware category.

4.4.5.5.4 key logger and spyware category.

4.4.5.5.5 P2P software category.

4.4.6 **Reports**

4.4.6.1 Support is needed for presentation of all system incidents, including management and administration actions and threats, in an up-to-date and historical display on an integrated dashboard that allows forensic evidence to be accessed and investigated.

4.4.6.2 A detailed account regarding the display and profiling capabilities of the system dashboard is required.

4.4.6.3 Support of a full audit trail, including ability to collect data on end-users’ and system administrators’ activity and integration with leading SIEM systems (in accordance with a Gartner magic quadrant), is required.

4.4.6.4 Support of standard- and regulation-compliant report creation is required, at least vis-à-vis the following:

4.4.6.4.1 PCI.

4.4.6.4.2 ISO.

4.4.6.4.3 SOX.

4.4.6.4.4 FISMA.

4.4.6.4.5 GLBA.

A detailed account regarding the way reports will be produced and additional standards supported is required.

* + - 1. Support of creation of existing and predefined reports, and of personally adjusted reports, is required.
      2. A detailed account is required regarding the existing array of reports in the system and the process of producing pre-adjusted reports.
      3. Support of production and export of reports, in the following formats at least, is required:
         1. .pdf
         2. Word.
         3. Excel.
         4. HTML.
         5. A detailed account is required regarding the timing of report production, their channels of dissemination, and additional formats supported by the system.
      4. Support of the ability to retain records for at least 12 months is required. Support of the ability to back up system logs and produce monthly reports is required.
      5. User management [NG: might something be missing in the source?]
      6. The solution shall support a central management array such as Active Directory for user authentication and licensing. Also, integration with PIM/PAM solutions shall be described in detail.
      7. Support including version upgrade, repair updates, including availability at Customer’s site where necessary, on the basis of the SLA requirements of the Tender, is required.
      8. The ability to establish volumes and quotas for download/upload and internet surfing quota limits for users/groups is required. A detailed account is required regarding the ability to establish volumes and quotas by means of the system, including blockage ability and/policy revision when a specified limit is reached.
      9. The ability to allocate a defined set of policies across several gateways is required.
      10. The system manager shall be able to enforce policy selectively for remote users (private and public government cloud) from the same management system.
      11. Support of protection against Zero Day attacks for migrating users is required.
      12. Support of protection against malware exploitation on browsers (e.g., HTML Smuttling) is needed and a detailed account is required regarding the way this shall be applied, the scan engines, and additional related capabilities.
      13. SSL supervisability over local and migrating users is required.
      14. The ability to determine authentication or to block untrusted certificates is required.
      15. The ability to access online and/or local databases in order to catalogue URLs as malicious or approved is required. A detailed account is required regarding SSL supervision, blockage, and Hostname/IP address monitoring on the basis of risk-score data.
      16. A detailed account is required regarding the number of categories supported by the secured Web access model. A detailed account is required regarding the number of categories to which an URL can belong. A detailed account is required regarding code-of-conduct-setting abilities on the basis of these categories.
      17. Support of personally adjusted categorization and of manual sorting of URLs into categories are required.
      18. The ability to make policy on the basis of predetermined and personally adjusted categories such as file-sharing, gambling, and so on, is required.
      19. Support of the following protocols is required:
          1. TLS.
          2. HTTP/3.
          3. HTTPS.
          4. DoH.
          5. IPv6.
      20. Support of full encryption between client and proxy servers is required. A detailed account is required regarding how support of one protocol and other protocols will be achieved.
      21. Support of signature-based malware detection is required.
      22. A detailed account regarding embedded sandbox engine is required s.
      23. Support of malware activity or Shadow IT activity is required. A detailed account regarding detection method and capabilities is required.
      24. Support of metadata exposure in regard to the cloud service to which the organization’s users have access is required:
          1. functionality (e.g., social media, file-sharing).
          2. geoposition of cloud service.
          3. jurisdiction of cloud service.
          4. known weaknesses of cloud service.
          5. encryption policy for data stored with cloud service.
          6. encryption protocols used for data transfer in cloud service.
          7. calculation of overall risk of cloud service. A detailed account is required regarding user’s ability to observe the parameters that lead to the risk calculation.
      25. Support of assessment of cloud-service compliance with the following standards/regulations is required:
          1. GDPR.
          2. PCI.
          3. ISO.
          4. CSA.
          5. HIPAA.

A detailed account regarding support of additional standards or regulations is required.

* + - 1. In the event of a security breach at a cloud-service supplier, support of reportage including details of the breach and information about use by staff of the breached cloud service is needed.
      2. A detailed account is required regarding information-leak prevention capabilities. A detailed account regarding the characteristics of this functionality, using and not using an agent, is required.
      3. Support for defining an alert as a false positive or a false negative for risk-engine optimization is required.
      4. Support for defining a watchlist to monitor selected users who detect [= who display?] suspicious behavior is required.
      5. Support of the ability to edit blocked pages is required.
      6. A detailed account regarding support of browser isolation is required. A detailed account regarding user/group-based isolation and additional isolation capabilities is required.

4.4.7 **Licensing**

4.4.7.1 The Bidder shall provide Enterprise Premium level licenses in order to cover all technical and functional requirements that appear in this Document.

4.4.7.2 The Bid shall include technical instructors for the product and a dedicated instructional array for system managers.

4.4.7.3 Licensing shall include the system required and the cloud services for its operation.

4.4.8 **Zero-trust network access, private access**

4.4.8.1 A detailed account regarding the way external users will connect to the system is required.

4.4.8.2 A detailed account is required regarding the product’s abilities to provide review capabilities at the following levels among others:

4.4.8.2.1 network level.

4.4.8.2.2 context-aware.

4.4.8.2.3 identity-based access.

4.4.8.3 A detailed account regarding the way the product lowers IT and communication costs is required.

4.4.8.4 A detailed account regarding protection against threats carried in ZTNA traffic is required.

4.4.8.5 A detailed account regarding the system’s ability to enhance the efficiency of processes such as routing and latency is required.

4.4.8.6 A detailed account regarding support of operating systems, including the following *inter alia,* is required:

4.4.8.6.1 Windows.

4.4.8.6.2 Mac.

4.4.8.6.3 Linux.

4.4.8.6.4 IOS.

4.4.8.6.5 Android.

4.4.8.7 Support of detection of managed and unmanaged components is required.

4.4.8.8 Support of geolocation-based blocking and alert capabilities is required. A detailed account regarding the ability to create a code of conduct and policy on the basis of geolocation information is required.

4.4.8.9 A detailed account is required regarding support of SaaS- or cloud-service manufacturers with which agreements allowing traffic optimization exist.

4.4.8.10 A detailed account regarding integration with SD-WAN technologies and suppliers is required.

4.4.9 **Cloud system information management and security (CASB) module**

4.4.9.1 The ability to track changes in policy and system definitions, including roll-back capability, is required.

4.4.9.2 The ability to review policy before applying it to the organizational environment is required.

4.4.9.3 A detailed account regarding the ability to supply a system for assimilation into an environment of checks is required.

4.4.9.4 Support of log files from different gateway origins, and from CLSF, CEF, and Syslog at the very least, is required.

4.4.9.5 In a proxy situation, service shall be able to integrate with every other organizational proxy with no need to create an additional hop.

4.4.9.6 Integration of the service/system with mobile devices shall not disrupt applications installed on said devices and that contain hardcoded URI.

4.4.9.7 The service/system shall contain a simple user interface with user-profile-based access authorizations.

4.4.9.8 System availability with a 0 recovery-time objective is required.

4.4.9.9 Support of growth ability including system users and devices is required. A detailed account is required regarding system ability to supply growth in hardware, software, and storage-volume requirements.

4.4.9.10 A detailed account is required regarding system performance and latency data in accordance with the way the system is assimilated.

4.4.9.11 A detailed account regarding characteristics of the CASB solution for cloud-based systems policy application is required.

4.4.9.12 Support of multiple secured links to cloud services via API interfaces is required.

4.4.9.13 Support of linkage to new cloud applications is required. A detailed account regarding SLA in the event of connection to a new cloud application is required.

4.4.9.14 Structured capability and manual definition capability relating to creation of different levels of access to data (RBAC) and defining applications, as the system manager shall determine, is required.

4.4.9.15 The ability to create a code of conduct on the basis of AD attributes is required.

4.4.9.16 Personally tailored enforcement of application access control, on the basis of various parameters including the following, is required:

4.4.9.16.1 device.

4.4.9.16.2 location.

4.4.9.16.3 user.

4.4.9.16.4 activity.

4.4.9.17 Integration with systems such as Microsoft Graph APIs to monitor users’ activity and enforce policy is required.

Detection and presentation of cloud platform data, applications, and infrastructures

4.4.9.18 Support of an integrative CASB solution, run by an integrated central-management system, is required.

4.4.9.19 Support of “Shadow IT” detection and presentation is required.

4.4.9.20 Support of detection and presentation of IaaS and PaaS services in use is required.

4.4.9.21 Support of detection and presentation of users of cloud applications on the basis of user name or ID is required.

4.4.9.22 Support of detection and presentation of specific instrument and browser for users of cloud applications is required.

4.4.9.23 Support of detection and presentation of information about geoposition and IP from which access is made is required.

4.4.9.24 Support of detection of stored or in-use data (files, fields) with undetected cloud services and presentation of the same as items of significant data risk are required.

4.4.9.25 Support of DLP policy creation even in the course of password-protected or locked/encrypted file upload to the cloud is needed in order to allow the CASB to supervise and protect critical data in cells, columns, document notes, and metadata. A detailed account is required regarding additional characteristics such as support of lexicons and data authentication mechanisms including personal ID information (PII), protected health information (PHI), ID card numbers, credit-cards, customer numbers, etc.

4.4.9.26 Support of data monitoring, using the API interfaces supplied by the cloud application and allowing the creation of an encryption policy or an alert against breach of use policy in various types of applications, is needed. A detailed account regarding interface capabilities and integration with cloud-system capabilities is required.

4.4.9.27 Support of flexible encryption-key management solutions is required, including keys managed in a local solution or a cloud-based HSM component.

4.4.9.28 Support of data monitoring by means of a proxy connection between users and the cloud application and creation of policies on blocking, encryption, or alert against breach of use policies in various types of applications, is required.

4.4.9.29 Support of checking of traffic sent by HTTPS and application of policy at time of proxy in-line assimilation are required.

4.4.9.30 Support of integration of ID tags from local or third-party applications and their incorporation into policies is required. A detailed account is required regarding the ability to integrate information from DRM/IRM information-rights management systems in order to prevent copying, printing, or dissemination of sensitive documents.

4.4.9.31 Support of location-based notifications relating to storage and integration into policy is required. The system shall support capabilities of compliance with, and satisfaction of, various jurisdictions’ requirements.

4.4.9.32 Integration with MDM systems is required. A detailed account is required regarding ability to make policy based on integration of an organizational MDM array and integration of unmanaged BYOD devices.

4.4.10 **Access control**

4.4.10.1 Support for classification and prioritization of cloud services and creation of an access-control policy based on a reliability level that the organization shall determine are required. Examples are “reliable” services that all users in the organization may access, “unreliable” services that are blocked at all times, and “not totally reliable” services that must be carefully supervised and controlled when a decision on a given cloud application is made.

4.4.10.2 Support of integration with organizational security infrastructure for management of the user ID array—be it internal or cloud-based—including single sign-on capability, is required.

4.4.10.3 Support of authentication technologies and protocols and of issuance of authorization is required. A detailed account regarding support of protocols such as OAuth, ADFS, SAML, and SCIM is required.

4.4.10.4 Strong, policy-based ID capability combining organizational, local, or cloud-based solutions is required. A detailed account is required regarding a given user’s ability to activate an event-based policy leading to a demand that the user provide an additional layer of ID.

4.4.10.5 Data ID support is needed, including, at the very least, user, device, location, service, network, time, and type of data, for the purpose of integration into code of conduct and policy.

4.4.10.6 Support of access control based on user’s actions and access reliability is required. Namely, insofar as, for example, the organization deems Google Drive “unreliable” and Microsoft OneDrive “reliable,” a user may download a document shared with him/her on Google Drive but cannot upload documents to that destination.

4.4.10.7 The ability to define and apply policy on the basis of user authorizations for use of cloud services is required, for example, permission to use an organizational Dropbox without being able to make personal use of the system.

4.4.10.8 The ability to define specific access-control requirements parsed by countries is required, e.g., allowing access to a CRM platform from the United States, Canada, and the European Union but blocking access from other countries.

4.4.11 **Management of cloud-service-provider risk**

4.4.11.1 The CASB supplier shall perform annual audits such as SOC II type 2. Information about the audit and its frequency shall be available on the user’s interface.

4.4.11.2 The system manufacturer shall provide a detailed account of compliance with additional standards and risk-assessment activities that it undertakes on a regular basis.

4.4.12 **Threat detection**

4.4.12.1 Support of a full audit-trail log is needed. A detailed account is required regarding data retained in the activity log and the duration of data storage.

4.4.12.2 The system shall include a behavior-analysis mechanism comprising, *inter alia,* monitoring of user activity and detection of deviations in favor of [??] use of code of conduct and policy.

4.4.12.3 Support of mechanisms for detection of suspicious accounts that may have been degraded and for automatic actions to repair said accounts, e.g., creating an alert and blocking access to a specific account, is required.

4.4.12.4 Support of transfer of deviations from policy to a predefined group of analysis for investigation is required. A detailed account is required regarding the ability to supply data to the incident-response team and the forensic teams after suspicious activity.

4.4.12.5 Integrability into IaaS suppliers’ management consoles is required in order to prevent damage that may affect applications operating on these platforms if a privileged-user (administrator) account is degraded.

4.4.12.6 The ability to produce anomalous detection alerts in the cloud services is required.

4.4.12.7 Support for monitoring data stored in cloud applications and detection of malware in files is required. Said capability shall be implementable in real time and in ad-hoc scanning coupled with API-based integrations.

4.4.13 **Reporting and alerts**

4.4.13.1 The ability to create and filter system reports (structured reports and personally adjusted reports) is required. A detailed account is required regarding the types of reports included in the system and an interface for the creation of adjusted reports.

4.4.13.2 The ability to send alerts to system managers and predetermined others, in real time and at specified times, is required. A detailed account regarding the system’s ability to send alerts (sending method, content, timing) is required.

4.4.13.3 Revision and Best Practice management. [Is something missing?]

4.4.13.4 A detailed account regarding Manufacturer’s Best Practices in assimilating the system is required.

4.4.13.5 A detailed account is required regarding the methodology of system update and the manner of update installation, in a way that will ensure that any change will be tested and approved before being assimilated in the production environment.

4.4.14 **Roadmap**

4.4.14.1 A detailed account regarding the Manufacturer’s roadmap in the domain of the specific Competition is required, focusing on main features and a schedule for the coming year.

4.4.15 **System infrastructure**

4.4.15.1 The system will be installed on the public cloud platform of one of the Winners—Amazon Web Services and Google (hereinafter: “**the Cloud Suppliers**”)—of Tender 01-2020 for the Provision of Cloud Services on a Public Platform for Government Ministries and Support Units (hereinafter: **“Nimbus Tender”**) in accordance with the following rules:

4.4.15.1.1 The system shall operate from a public-cloud region that one of the cloud providers has set up within the territorial confines of the State of Israel as is approved by the Administrator of the Tender (hereinafter: **“the Israeli Region”**) no later than 12 months after the day on which the winning candidate is announced.

4.4.15.1.2 If the Israeli Region of the cloud provider on the basis of whose cloud the system is offered has not yet been set up, the system shall be supplied, provisionally and until the Israeli Region is set up, on the basis of the largest public cloud region operated by the cloud supplier in which the proposed system operates within the confines of the European Union (hereinafter: **“the Overseas Region”**). In this case, the supplier shall transfer the system, including the users’ data, to the Israeli Region within six months of the day on which the cloud provider certifies that the Israeli Region is prepared for operation of the system in accordance with requirements from the Supplier. The users’ data shall be transferred in coordination with the Customers and at no added cost.

4.4.15.1.3 The system shall comply with all requisite standards and with the SLA within twelve additional months, at the latest, from the day on which the system begins to be supplied in the Israeli Region.

4.4.15.1.4 A detailed account regarding the configuration of the system, with reference to the following matters, is required:

4.4.15.1.4.1 the public cloud infrastructures on which the solution is based, among the cloud provider’s platforms;

4.4.15.1.4.2 whether the account on which the system operates is dedicated to the system offered or is shared by all Customers.

4.4.16 **Working configuration of the proposed system**

4.4.16.1 A detailed account regarding the working configuration of the proposed system is required, with reference to the following points:

4.4.16.1.1 the place where protected information is kept—on a “network” (e.g., VPC) of the Customer, with the Supplier, with the Manufacturer, or somewhere else. If the information is not kept with the Customer, a detailed account of the place where it is kept, including the state and the entity in which the knowledge is kept, is required.

4.4.16.1.2 the place where Content Data (as defined below) are processed—on a “network” (e.g., VPC) of the Customer, with the Supplier, with the Manufacturer, or anywhere else. Insofar as the Content Data are not processed with the Customer, a detailed account of the place where they are kept, including the state and the entity in which the data are kept, is required.

4.4.16.1.3 If the material and the processing are with the Customer, a detailed account of the Supplier’s or the Manufacturer’s ability to access or control the information or the system, if such exists, is required.

4.4.16.1.4 A detailed account regarding the configuration of system connection to the Customer’s network is required, with reference to the following points:

4.4.16.1.4.1 how the Customer’s network in the cloud is connected (e.g., VPC); a detailed account is required regarding whether the connection uses, for example, a peering, VPC endpoint, or private-link configuration, or is represented on the Customer’s network itself either via a VPN link or in some other way; how the link is secured; and whether external addresses need to be opened in order to connect to the service;

4.4.16.1.4.2 the interface with the management system of the service: a detailed account is required regarding whether the connection uses, for example, a peering, VPC endpoint, or private-link configuration, or is represented on the Customer’s network itself either via a VPN link or in some other way; how the link is secured; and whether external addresses need to be opened in order to connect to the service.

4.4.17 **Human-capital security**

4.4.17.1 A detailed account is required regarding the control, authentication, and screening of staff of the Manufacturer and its subcontractors, with reference to differences commensurate with types of staff and levels of risk intrinsic to their roles.

4.4.17.2 A detailed account is required regarding training and refresher activities relating to security, safety, and cyber procedures for staff of the Manufacturer and its subcontractors.

4.4.17.3 A detailed account is required regarding training and professional certification processes undergone by professional staff of the Manufacturer and its subcontractors.

4.4.17.4 A detailed account is required regarding supervision mechanisms for compliance with procedure and handling of breaches of security procedures or other critical procedures.

4.4.17.5 A detailed account is required regarding the use, if any, of tools to detect human risks (e.g., exceptional behaviors, managers’ or peers’ feedback in response to problems, etc.) emanating from holders of sensitive positions or those with high levels of access authorization.

4.4.18 **Supply-chain security**

4.4.18.1 A detailed account is required regarding the standard by which the supply chain is secured, such as NIST SP 800-53 Rev. 5/Nist, SP 800-161 Rev. 1, ISO 28000, or some other international standard; the internal procedure, if any, shall be attached.

4.4.18.2 A detailed account of the means used to secure the supply chain is required, including the following:

4.4.18.2.1 control processes over insertion of software and software updates from an external source, including detection of weaknesses, backdoors, and embeddings with malicious capabilities.

4.4.18.2.2 control processes over insertion of software and software updates from an internal source, including detection of weaknesses, backdoors, and embeddings with malicious capabilities.

4.4.18.2.3 Every additional relevant process or control shall be described in detail.

4.4.18.3 A detailed account is required regarding the process of supervision and control of subcontractors, including the standards by which said control is implemented.

4.4.19 **Information retained by the Manufacturer**

4.4.19.1 A detailed account is required regarding information retained by the Manufacturer in the course of service delivery, such as Processing Data (as defined below) and Subscription Data (as defined below).

4.4.19.2 A detailed account is required regarding the information-retention policy and the mechanisms used to delete information where necessary.

4.4.19.3 Insofar as the Supplier or the Manufacturer retains data, a detailed account is required regarding the means of protecting the information and the tools and processes that are meant to prevent unauthorized access to the information.

4.4.19.4 A detailed account is required regarding the process of allowing access to said data, the user groups authorized to view the information, and the control processes for detection of authorization abuse.

4.4.20 **Configuration security and modification management**

4.4.20.1 The Manufacturer shall act in accordance with a systematic policy on configuration management and modifications of all systems involved in delivering the Services, in compliance with accepted and requisite standards.

4.4.20.2 A detailed account is required regarding the standard by which said processes are performed, if any, including a description in principle of configuration control systems and the process of control, certification, and documentation of modifications.

4.4.20.3 A detailed account is required regarding controls meant to prevent unapproved downgrade of encryption mechanisms, key-management mechanisms, and protective systems and services, if any.

4.4.20.4 A detailed account is required regarding the way development processes are protected and controlled, such as via a secure development process (SDLC) and relevant standards, insofar as the Manufacturer complies with them.

4.4.21 **Limitation of support access**

4.4.21.1 A detailed account is required regarding the system-support process, the identity of support providers, whether they represent the Supplier, the Manufacturer, or the cloud provider, and the process applied by the Supplier and the Manufacturer in case of need for said access, including internal authorization paths, authorization processes with the Customer, security of access, and documentation of access (including keeping a log, recording sessions, and so on).

4.4.21.2 A detailed account is required of whether a mechanism in which every support access to components that the Customer uses and that accommodates or facilitates access to processing data is applied only pursuant to a defined authorization process that entails authorization from the Customer’s representative for support access.

4.4.22 **Risk management**

4.4.22.1 If the Manufacturer has an information-security manager who is in charge of securing information about the products offered, a detailed description is required regarding his or her job and whether he or she is a member of the Manufacturer’s board of directors.

4.4.22.2 A detailed account regarding the Manufacturer’s risk-management processes is required.

4.4.22.3 A detailed account of the parties that implement these processes, levels of supervision, levels of escalation in handling issues, and the way untreated findings are handled, is required.

4.4.22.4 A detailed account is required regarding the tools, means, and manner of implementation for facilitating dynamic risk management tailored to changes in the contours of threats and the delivered services.

4.4.23 **Identification for the Service offered**

4.4.23.1 The Service shall support standard ID protocols such as OAuth, Open ID, and SAML for single sign-on to the Customer’s systems and support of multifactor authentication. A detailed account regarding ID protocols supported (such as U2F, FIDO, and OTP) is required.

4.4.23.2 A detailed account regarding interfacing with IdP/IAM tools for user and third-party ID management is required. [Susan: the gerund התממשקות refers to the act of interfacing and IdP/IAM are the tools with which it’s done.]]

4.4.23.3 A detailed account regarding support for individual granting of access at the RBAC (role-based access control) and ABAC (attribute-based access control) levels is required.

4.4.23.4 The Service shall support receipt of users’ particulars from a central ID system using standard protocols.

4.4.24 **Survivability and business continuity (SLA) of the offered service**

4.4.24.1 The SLA of Service provided from the Israeli Region shall not be inferior to the SLA of Service in any other region. Data on the uptime that the Manufacturer undertakes to provide shall be explained in detail.

4.4.24.2 A detailed account is required regarding the mechanisms that ensure Service and information survivability, including system deployment among different locations, the manner of information backup, backup integrity maintenance, recoverability testing, resilience in various failure scenarios, and so on.

4.4.24.3 If backups outside the cloud environment are made, a detailed account shall be made regarding the mechanism that verifies destruction of memory platforms and components that reach end-of-service (such as removal from the system, replacement, or malfunction).

4.4.24.4 A detailed account is required regarding the Manufacturer’s way of controlling the quality of service delivered from the public-cloud region and the level of escalation specified in its procedures.

4.4.24.5 It shall be possible to back up or export system data to the Manufacturer-controlled platform on a regular basis. A detailed account is required regarding backup format and its compatibility with standard systems in the market.

4.4.25 **Protection of Service infrastructure**

4.4.25.1 The Manufacturer shall operate an SOC that provides 24/7 (24 hours per day, 365 days per year) cyber monitoring of its systems. A detailed account is required regarding the capabilities of the SOC operated by the Manufacturer, the SIEM system that the Manufacturer uses, and additional components and capabilities that the SOC uses in its regular activity. Insofar as the Service is operated by a subcontractor of the Manufacturer, its details shall also be noted.

4.4.25.2 A detailed account is required regarding the use of protective measures for endpoints (EPP/EDR/XDR) in the Manufacturer’s environment. If it exists as a service operated by a subcontractor of the Manufacturer (MSSP), its details shall be reported as well.

4.4.25.3 A detailed account is required regarding the use of automation tools to monitor and deal with incidents. A detailed account is required regarding the Manufacturer’s operating methodology (such as SOAR), the relevant tools, and the way they are implemented.

4.4.25.4 Incoming and outgoing traffic to/from the service infrastructure shall be monitored for detection of attacks or suspicious activity. A detailed account regarding the Manufacturer’s capabilities in this respect and the working processes that it invokes for this purpose is required.

4.4.25.5 The Manufacturer applies monitoring and working processes in a Privacy by Design configuration that minimizes exposure of information to human players. A detailed account regarding the tools and methods that the Manufacturer applies to implement these processes is required.

4.4.25.6 If the Manufacturer uses tools that provide continual monitoring of the attack surface of its infrastructure (attack surface management), a detailed account regarding all tools and working processes used is required.

4.4.25.7 A detailed account is required regarding the means used to protect the systems that deliver the Services against unauthorized modifications and the monitoring measures that the Manufacturer invokes for control of said means.

4.4.25.8 The Manufacturer provides all relevant security updates for all infrastructures, systems, and services offered. A detailed account regarding the updating processes and the frequency of updates is required.

4.4.25.9 All users who can access information of Customers and all holders of privileged access, such as administrators, operators, support personnel, and DevOps, shall be subject to high-level monitoring and identification. A detailed account regarding the working processes and tools that are invoked for this purpose is required.

4.4.25.10 A detailed account regarding the way system users’ subscription data are protected, including control of access thereto, their encryption, and security tools against unauthorized access or leakage is required.

4.4.25.11 A detailed account regarding the way system-management interfaces are protected, users are separated, and access is denied to unauthorized players including Supplier’s employees, Manufacturer’s employees, and Manufacturer’s subcontractors, is required.

4.4.25.12 A detailed account regarding the way the system’s internal and external APIs are protected, is required.

4.4.26 **Security tools used to protect the offered Services**

4.4.26.1 A detailed account is required regarding advanced and automatic analytical tools, including those in which AI capabilities are integrated, to detect suspicious activity in users’ services, any exposure or attempt to expose sensitive information, and so on.

4.4.26.2 **A detailed account** is required regarding additional cyber control, monitoring, and protection tools that the Manufacturer uses and that Customers may use to better protect the information in their possession, such as DLP capabilities, coping with malicious code, and so on.

4.4.27 **Encryption and key management in the offered Services**

4.4.27.1 A detailed account regarding information encryption methods used at the various levels of service is required.

4.4.27.2 All system data shall be encrypted at rest and in transit as the default. Insofar as the Supplier considers said encryption inapplicable, this shall be explained in full detail including compensatory controls, if any.

4.4.27.3 A detailed account is required regarding the encryption types and algorithms that the Manufacturer uses in its services, such as at-rest encryption, in-transit encryption, and runtime encryption; the standard on which they are based; and outside confirmation of algorithmic and protocolic encryption resilience.

4.4.27.4 A detailed account regarding way keys are managed and saved in reference to each tier and type of service delivered is required.

4.4.27.5 A detailed account regarding interface support for the key-management infrastructures with which the Manufacturer interfaces (such as KMS) is required.

4.4.27.6 If the Manufacturer operates an independent key-management infrastructure, a detailed account regarding the proposed solution, with emphasis on full compliance with FIPS-140-2 Level 2 or higher, is required.

4.4.27.7 A detailed account is required regarding the system’s ability to work in a Bring Your Own Key configuration, including the ability to protect and toughen the system and the user’s ability to control the various parameters of the encryption keys.

4.4.27.8 All processes of defilement, modification, replacement, and revocation of keys, **and any other action related to encryption keys**, shall be performed by the Customer such that neither the Supplier, nor the Manufacturer, nor any other party unauthorized by the Customer may view or access it (beyond systems that require access to a key for the delivery of the Service).

4.4.28 **Log collection and monitoring**

4.4.28.1 The Customer may receive all data related to processing and access to its systems with support for forwarding the data to the Customer’s SIEM system, the Administrator of the Tender, or a third party. A detailed account is required regarding the way logs are sent (online interface, periodic transfer of files, API, and so on) to supported SIEM systems (such as Chronicle and QRadar) and the extent of support.

4.4.28.2 A detailed account regarding possible origins of a log (such as infrastructure, applied infrastructure, application, information security, and so on) is required.

4.4.28.3 A detailed account is required regarding currentness of information (time from occurrence of incident to transfer of information), extent of information, investigation capabilities of Customer or Customer’s agent, and so on.

4.4.28.4 A detailed account is required regarding the amount of time in which the Manufacturer retains processing Data and subscription Data, the Manufacturer’s policy on retaining these data, and the way said data are protected.

4.4.29 **Investigation**

4.4.29.1 A detailed account is required regarding the Manufacturer’s capabilities, tools, and working processes relating to investigation of and response to cyber incidents in its systems.

4.4.29.2 A detailed account is required regarding the process of operating incident-response arrays, if any, in the event of investigation of a security incident; involvement of the cloud provider; response times; resources accessible to the Customer, interface configuration, and so on.

4.4.30 **Internal control and compliance with standards**

4.4.30.1 The Service shall comply with at least one of the following standards:

4.4.30.1.1 ISO 27001.

4.4.30.1.2 SOC 2 AICPA.

4.4.30.1.3 The standard with which the Service complies shall be specified in detail.

4.4.30.1.4 Additional standards with which the Service complies, such as ISO 27017, ISO 27018, CSA STAR Level 2, and so on, if any, shall be specified in detail.

4.4.30.2 A detailed account is required regarding the organization’s working process and the systems/tools used by the Manufacturer to verify service compliance with all rules and standards to which the Manufacturer is committed.

4.4.30.3 A detailed account regarding levels of supervision, levels of escalation in handling issues, and the way untreated findings are handled is required.

4.4.31 **Tenant separation and compartmentalization**

4.4.31.1 A detailed account is required regarding the Manufacturer’s ability, if any, to isolate and segregate one tenant or another, with reference to the following points:

4.4.31.1.1 The manner of separating and segregating shared services and means of preventing information leakage among tenants, access of a given tenant’s users to another tenant’s resources, separation of management and control, and so on.

4.4.31.1.2 The ability to prevent access by a given tenant’s users to resources of another (foreign) tenant unless such access is approved, even if the user is authorized to access the foreign tenant’s resources. Preventive capabilities not based on the ID system shall be specified in detail.

4.4.31.1.3 The ability to prevent access by foreign tenant’s users to a tenant’s resources unless such access is approved, even if the foreign tenant is authorized to access the tenant’s resources. Preventive capabilities not based on the ID system shall be specified in detail.

4.4.31.2 The ability to generate a dedicated and personal address (IP or URI) for users of a tenant or a group of customers, that is not shared with other tenants.

**5. Appendix D—Reference Model**

5.1 All prices shall include a warranty as mandated in Chapter 3 of the Central Tender Documents and as specified above in the Specific Invitation Documents.

5.2 The Bidder shall enter its bid, at the prices expressed in the official list prices, into the Excel worksheet attached as Appendix D1 to the Notice of Promulgation of Specific Invitation.

5.3 The prices in the Dynamic Online Specific Invitation shall be determined in accordance with the provisions specified above.

**5.4 Installation, assimilation, and maintenance services**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Section** | **Qty. for weighting** | **Maximum rate (incl. VAT)** | **Remarks** |
| A. | Annual maintenance price, in percent of actual product price (from Year 2 onward) | 4 | 20% | Total 5 years for weighting in Specific Invitation |

**5.5 Remarks**

5.5.1 Each Bidder shall make a real procurement commensurate with the number of users that it needs. If the Manufacturer’s price includes a price for personal licensing and by price levels commensurate with the number of users for which licensing is procured, the licensing price for each number of users shall accord with the Supplier’s price for an individual license at the level of 50,000 licenses or the actual size of the order, whichever is lower. All the foregoing shall follow application of the discount that shall be set at the end of the Specific Invitation. The foregoing shall be valid for all products and services that may be procured, including those added during the Term of the Contract.

5.5.2 If the product is procured on the basis of a Subscription pricing model, the following model shall be used to calculate the cost:

5.5.2.1 The annual subscription price shall be multiplied by 5—in accordance with the calculation horizon in the Specific Invitation as specified above*.* That is, the total procurement and maintenance cost shall be priced against a comparison period of 5 years.

**For example,** if the one-year subscription price for a given component is $100, the opening price of the total cost for five years for said component shall be $500, and said cost shall include all procurement and maintenance costs for said period.

5.5.2.2 For the purpose of the Dynamic Online Specific Invitation, and insofar as the maintenance price must be noted, the maintenance price shall be set at 20% of the procurement price **and shall not be weighted in calculating the Bid price**. This component shall affect neither the price nor the discount rate.

5.5.2.3 The discount rate off the annual subscription price that shall be set at the end of the Specific Invitation shall be in effect each year in which the Customer shall procure it, even after the fifth year. Said price shall include all procurement and maintenance costs, as stated in Section 1.5.3.3 above*.*

1. **Appendix E—Manufacturer’s Affirmation**

**This Affirmation may be signed in Hebrew or in English**

**Manufacturer’s Affirmation**

**Attn:**

**Government Procurement Administration, Division of the Accountant General, Ministry of Finance**

Re: Specific Invitation no. 5 for the Provision of SSE—Secure Service Edge—and Related Services, promulgated within the framework of Central Tender 05-2022 for the procurement and delivery of products and services in the field of information security and cyber protection for government ministries and support units (hereinafter: **“the Specific Invitation”**).

I, the undersigned, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, from \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, Ltd., which owns the intellectual property of the products and services offered in the Specific Invitation (hereinafter: **“the Manufacturer”**), by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter: **“the Bidder”**), hereby affirms the following:

1. The Bidder that in the Specific Invitation is offering products and services that we manufacture, is authorized by the Manufacturer to sell, install, and service the products and services in the domain of the Specific Invitation in Israel as an authorized agent of the Manufacturer, for a period of at least 12 months before the deadline for bid submission in the Specific Invitation.
2. The Bidder is *(check the appropriate box):*

an authorized supplier of ours in Israel for the offered products and services;

our company (the Manufacturer) or our subsidiary in Israel.

3. The Bidder holds the Manufacturer’s highest certification in the domain of the Specific Invitation and is authorized by the Manufacturer to sell the Service and commit to the requirements of the Tender and the Specific Invitation for the Service.

4. The Manufacturer confirms that it is familiar the terms of the Tender and the Specific Invitation.

5. The Manufacturer undertakes:

5.1 that, to the best of its knowledge, there is nothing to prevent the Bidder in the Specific Invitation from supplying the products and/or delivering the services of the Manufacturer under the terms of the Tender for the entire Specific Invitation period, including the optional periods included therein.

5.2 to provide the Bidder in Israel with full support in supplying and making available to the Bidder in the Tender the Manufacturer’s services and/or products so that it shall satisfy the terms of the Tender; to ensure that the services meet the requirements of the Tender and the Specific Invitation; to supply and make available expert and trained personnel, to establish an escalation mechanism from the Supplier to itself; and to help to maintain continuity in honoring the warranty for the products that it manufactures, all of which for the entire Specific Invitation period, including the optional periods included therein.

5.3 The terms of the Service shall be those specified in the Tender Documents and the Specific Invitation Documents. In the absence of an explicit or implicit instruction in the provisions of the Agreement or the Tender, the standard and public service agreement that the Manufacturer uses in the overseas region for customers of the size of the Government of Israel shall apply.

5.4 The Service shall be operated in the Israeli Region in accordance with Section 4.4.15.1 of the Specific Invitation Documents and in the accepted configuration of the Service in other overseas regions where the Service is deployed.

5.5 The response to Appendix C of the Specific Invitation is made in a manner concordant with the characteristics of the Service and the manner of its delivery by the Manufacturer.

5.6 The Manufacturer undertakes that in anything the Bidder must do that entails the Manufacturer’s assistance, the Manufacturer will provide all said assistance.

5.7 The Manufacturer will do everything necessary for the Bidder to honor the terms of the Tender, and of the Agreement executed by force thereof, that the Manufacturer must perform for the purpose of delivering the Service, during the entire the Term of the Contract.

5.8 In the event that the Bidder is incapacitated from continuing to deliver the Service, the Manufacturer or its representative shall assist in switching the delivery of the product and the Services to a new supplier whom the Administrator of the Tender shall determine.

5.9 To immediately apprise the Bidder and the Administrator of the Tender of items that may reach the end of their production, sale, or service cycle (End of Sale, End of Life, or End of Support) or that have already been declared as such.

5.10 Not to publish any information about the Bidder’s winning of a certain Specific Invitation without the prior approval of the Administrator of the Tender.

Name of Manufacturer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Position of signatory for the Manufacturer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature and stamp: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Manufacturer's Declaration for a Specific Invitation

**To:**

**Israel Government Procurement Administration (IGPA), Accountant General, Ministry of Finance, Israel**

**Re**: **Specific invitation number 4 for the supply of Secure Service Edge (SEE) systems and accompanying services, published as part of Central Tender 05-2022 for the Procurement and Supply of Cyber Security Products and Services for the Government Ministries and Additional Government Units] (hereinafter: the "Specific Invitation")**

I the undersigned, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, of the company \_\_\_\_\_\_\_\_\_\_\_\_\_\_, which owns the intellectual property of the products and services offered in the Specific Invitation (hereinafter: the "**Manufacturer**") by the Bidder \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (hereinafter: the "**Bidder**"), having been advised that I must tell the truth and that I will be subject to the penalties stipulated by law if I fail to do so, hereby declare that:

1. The Bidder, offering the products and services manufactured by us in the domain of the Specific Invitation, is currently authorized by us for the sale, supply, install and service of our products and services in Israel for at least the last twelve (12) months before the Specific Invitation submission deadline.
2. The Bidder is [check appropriate box]:

A licensed supplier/authorized reseller of the Manufacturer for the services and products offered.

The manufacturer or a subsidiary of the Manufacturer in Israel.

1. The Bidder is certified by us, the Manufacturer, at the highest certification level available for the offered product line, and holds the full rights to sell the service and to commit to the requirements of the Tender and the Specific Invitation.
2. The Manufacturer confirms it is familiar with the terms of the Tender and the Specific Invitation.
3. The Manufacturer undertakes a commitment to:
   1. That to the best of its knowledge, there is nothing to prevent the Bidder from supplying the products and/or services of the Manufacturer in accordance with the terms and conditions of the Tender for the entire duration of the Specific Invitation period, including the optional periods.
   2. Provide full support to the Bidder in Israel, to supply to the Bidder with products and services needed to fulfill the Tender, ensure that the services meet the requirements of the Tender and the Specific Invitation, and to provide support of skilled and experienced personnel and continuous Warranty for the products and services manufactured by it, and establishing an escalation process from the Bidder to it, for the entire Specific Invitation period, including the optional periods.
   3. The terms of the service will be the terms specified in the Tender and the Specific Invitation. In the absence of an explicit or implicit provision in the provisions of the agreement or the Tender, the standard and public service agreement of the Manufacturer which is used in the overseas region for Customers of the size of the Israeli Government will apply.
   4. The service will be operated in the Israeli Region in accordance with the provisions of section 4.4.15.1 of the Specific Invitation Documents, and in the accepted configuration of the service in other overseas regions where the service is deployed.
   5. The response to Appendix C ("ג") of the Specific invitation is made in a manner consistent with the characteristics of the service and the manner of its delivery by the Manufacturer.
   6. The Manufacturer undertakes that whatever is required from the Bidder plus the required assistance of the Manufacturer for the realization thereof, the Manufacturer will provide all the aforesaid assistance.
   7. Do all in its power to provide continuous warranty for the products and services manufactured by it, among other things, by cooperating with the transfer of sales and warranty for the products and/or services to another supplier which will be determined by the IGPA, including in the event that the Bidder or the Manufacturer will not be able to continue to supply the products and/or services.
   8. Immediately inform the Bidder and the IGPA about products and services which are at the end of production, sale or service and support cycle (End Of Life, End Of Sale or End Of Support).
   9. Not to publish any information regarding the Bidder's win with respect to any specific invitation published as part of this Tender.

[All terms—as defined in the Tender]

|  |  |
| --- | --- |
| Name of Manufacturer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Position with Manufacturer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Signature and seal: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

**7. Appendix F—Request for Confidentiality of Bid Details**

7.1 If the Bidder believes that its Bid contains sections that constitute a trade secret or a professional secret, it shall fill in the table below.

7.2 A Bidder that claims that certain parts of its Bid are a trade secret or a professional secret, or for any other reason mentioned in the Mandatory Tender Regulations, shall be enjoined against demanding the ability to view this part of the Winning Bid in the Individual Invitation.

7.3 It is stated for clarity that:

7.3.1 The Bidder’s response to the Reference Model (Appendix D1), including names of items, serial numbers, and description of items, prices, and quantities, **shall not be considered** a trade secret or a professional secret.

7.3.2 The Bidder’s response to the technical requirements (**Appendix C**) shall be considered a trade secret or a professional secret and the right to view this part of the Winning Bid in the Individual Invitation shall not be given.

|  |  |  |
| --- | --- | --- |
| **No.** | **Section/chapter of the Individual Invitation Document** | **Rationale** |
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |
| 4. |  |  |
| 5. |  |  |
| 6. |  |  |
| 7. |  |  |
| 8. |  |  |
| 9. |  |  |
| 10. |  |  |

**\* Additional lines may be added to the table, following the format above.**

**8. Appendix G—The Dynamic Specific Invitation System  
The Merav System**

8.1 This Appendix is meant to augment the contents of the Central Tender Documents and not to derogate from them.

8.2 This Appendix is meant for the Dynamic Online Specific Invitation stage and is an integral part of the Central Tender Documents and the Specific Invitation Documents.

8.3. In this stage—that of the Dynamic Online Specific Invitation—the Bidders will participate in accordance with Section 1.4.3 above and the rules specified therein.

8.4. The documents needed for the Dynamic Specific Invitation are specified in Appendix 2 of Booklet 2 of the Central Tender Documents.

8.5 **Registration for the National Identification System (once only)**

8.5.1 A bid may be submitted only by a party that has a user name with the National Identification System.

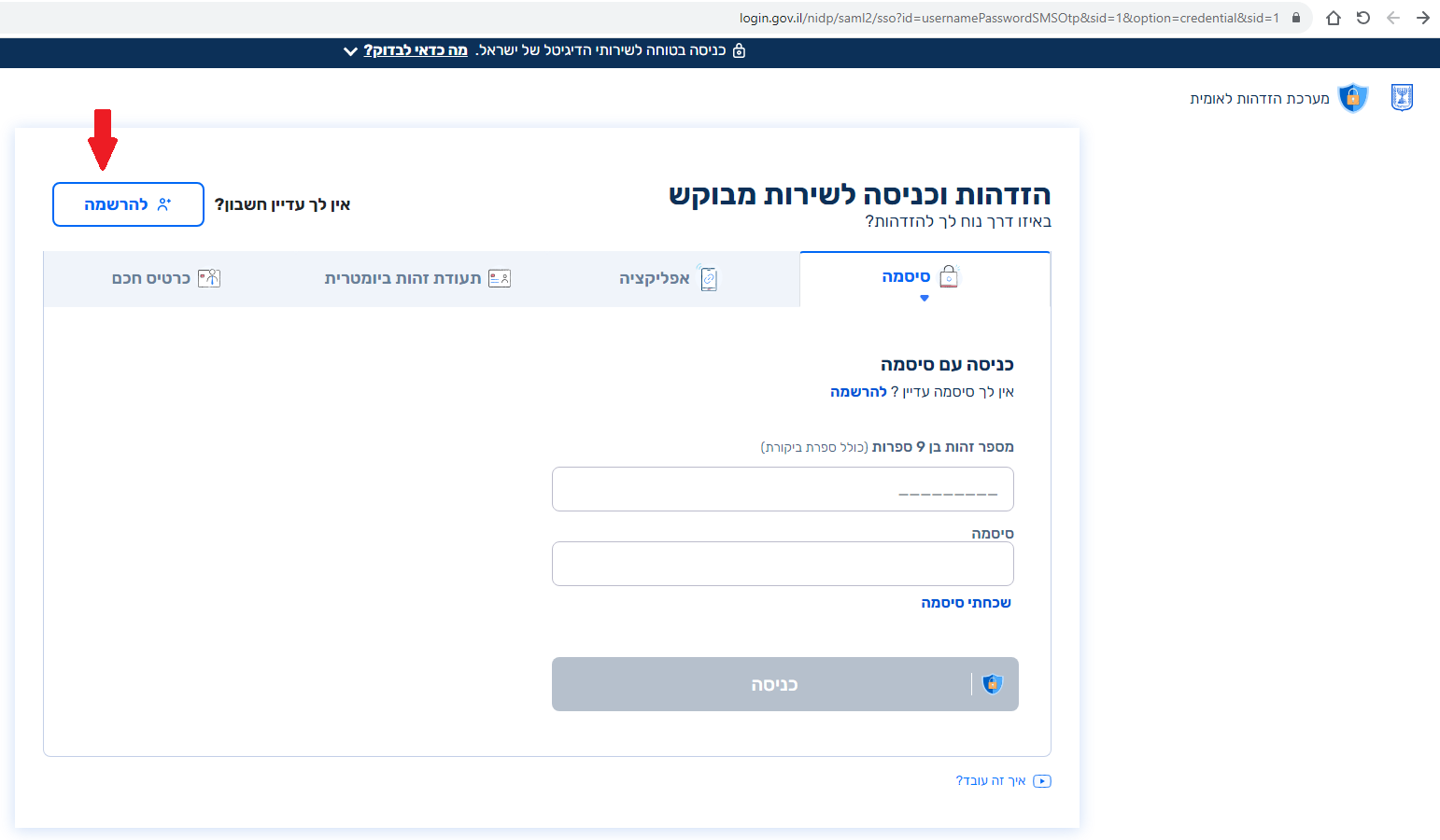
8.5.2 To register with the National Identification System, use the following link:

<https://account.gov.il/sspr/public/newuser>

8.5.3 Below is an instructional video that explains how to register with the National Identification System:

<https://www.youtube.com/channel/UCEflHGPEj-M7jtQ0PdzUZkQ>

8.5.4 The registration and ID process for various government systems, such as Merav, is carried out by means of the National Identification System. To register with the system, use a private electronic-mail account (such as Gmail) as shown in the image. For your information, registration also gives you access to various government services for your personal needs.



8.5.5 If you encounter a malfunction in the process of signing up for government identification or in the identification process itself, contact the system’s support hotline (Tel. 1299, [moked@mail.gov.il](mailto:moked@mail.gov.il), additional Tel. 08-6863100).

[Susan: from here to the end of the Appendix, the subsection numbering in the source file is mangled. I’ve left in place the numbering from the previous Specific Invitation]

8.6 **The Dynamic Online Specific Invitation**

8.6.1 Within the framework of the Specific Invitation, the Bidders shall compete in offering the best price to the Administrator of the Tender for the requisite equipment, products, and services in the domain of the Tender.

8.6.2 The bid that the Bidder shall present in the specific invitation shall be final and shall include all cost components of the sought-after products and services as are needed for their delivery and performance.

8.6.3 The bid in the Specific Invitation shall be binding upon the Bidder insofar as it wins, as specified in the Central Tender Documents and the Specific Invitation Documents.

8.7 **Reference model price**

8.7.1 Before the date of the Specific Invitation and 14 business days before the Dynamic Online Specific Invitation at the latest, Bidders shall present the Reference Model and the simulator with the Manufacturer’s list prices as of the submission date, in accordance with the quantities list specified in the Reference Model.

8.7.2 If, in the opinion of the Administrator of the Tender, a material change has occurred in the Manufacturer’s official basic price list, including a material change in the configuration of the equipment and the services, the Administrator of the Tender may ask for an update of the Reference Model accordingly.

8.7.3 The Bidder undertakes to advise the Administrator of the Tender at once if it discovers a material change in the Manufacturer’s basic price list or in the product line after it submitted its Bid and before the Specific Invitation took place. It shall also apprise the Administrator of the Tender of any product that, in accordance with a statement from the Manufacturer, may be approaching the end of its production, sale, or support (End of Sale, End of Life, or End of Support) or has already been declared as such, all of which as specified in the Main Tender Booklet.

8.7.4 The Administrator of the Tender shall conclude, for each Bidder in the final group of Bidders that are authorized to participate in the Specific Invitation, a Bid price in accordance with the Reference Model, to be calculated in New Israel Shekalim (NIS), at the representative foreign-currency exchange rate as shall be promulgated by the Bank of Israel seven days before the date of the Dynamic Online Specific Invitation, and shall add thereto Value Added Tax at the lawful rate insofar as the Bidder is liable to Value Added Tax (hereinafter: **“the Reference Model Price”**). The Reference Model Price shall be the maximum price for the opening bid of each Bidder in the Dynamic Online Specific Invitation.

8.7.5 The Reference Model price shall be sent on to the Bidder before the Specific Invitation for the purpose of review against the possibility of an arithmetic error in the conversion performed by the Administrator of the Tender. It is stated for clarity that the calculation in question is a technical one and that the Bidders in the Tender, at this stage of the Tender, shall not be allowed to revise any detail in their Bid.

**9. [In the source file, it is numbered 6] Appendix H—Information Processing   
and Security and Cyber Defense in the Services**

**9.1 Definitions**

9.1.1 **Security incident**—an incident that may impair the availability, reliability, or secrecy of protected information or the Services that the Customers use, including cyber attack.

9.1.2 **Digital instruction**—an instruction given by means of a configuration such as the Supplier’s management interface, APIs, or any other medium that is made available to the Customer.

9.1.3 **Protected information**—processing, subscription, and content data.

9.1.4 **Subscription data**—any information of users and Customers that is needed for subscription management, service delivery, or execution of charges.

9.1.5 **Processing data**—any information created in the systems of the Supplier or of the Manufacturer in the course, or as the result, of the processing of content data (metadata and logs) that may be attributed in some manner to the Customer, a group of Customers, or a user, and, within this generality—user IDs and particulars (including name, address, charging details, date of birth, electronic-mail address, telephone number), dates and times of login and logout, information about Customers, services that they operate, configuration data and files, actions taken in the various systems, usage details, IP addresses allocated by service providers (access data), transactional data, and traffic data, including geolocation of data source and destination, data size, data structure, path, and communication protocol.

9.1.6 **Content data**—digital data including any information, file, database, software, telemetry, logs, code, logic, datum, report, flag, text, picture, audio, video, image, and so on, in any format, that are uploaded, created directly by, or created at the request of, the user in the system of the Supplier or the Manufacturer, including in third-party services that the Supplier or the Manufacturer use.

9.1.7 **Information processing**—an action or a series of actions carried out with information, whether or not by automatic means, such as collecting, recording, organizing, structuring, storing, sharing, adjusting or revising, retrieving or recovering, using, encrypting, diffusing, or posting for viewing in any other way, adjusting or integrating, restricting, deleting or destroying, and so on.

9.1.8 **Cyber attack**—a security incident meant to overcome or circumvent means of protection or control that the Supplier, the Manufacturer, or the Customer use, or to exploit an existing weakness in an attempt to disrupt service or to destroy, lose, leak, modify, use, expose without authorization, or give access to protected information.

9.1.9 **Service Level Agreement** (hereinafter: **“SLA”**)—an agreement between a service provider and an end user that specifies the level of service that the service provider is expected to deliver and sets compensation for deviation from said level.

**9.2 Mandatory information security and cyber defense**

9.2.1 Without derogating from the Supplier’s obligation anywhere else, the Supplier shall be responsible for preserving, protecting, and maintaining the integrity of protected information in its systems and shall not access it, allow another to access it, use it or change it in any way, and allow any use or change, by commission or omission, that is not allowed under the provisions of Israel law and the provisions of this Agreement and this Appendix.

9.2.2 The Supplier is responsible for ensuring that Customers and users receive regular access to the protected information and, in any event, not be denied access to said information in a way that contravenes the provisions of this Agreement or of Israel law.

9.2.3 The Supplier understands that the protected information includes information about working processes of the Government of Israel and information that, in part, pertains to Israel citizens and residents. Accordingly, any exposure, impairment, damage, denial of access, or loss of information, or exposure of information to a third party, is liable to cause grievous damage to the Administrator of the Tender, Customers, and users, as well as to third parties, and the Supplier shall safeguard the protected information in compliance with the highest standards that exist in the market and shall not share it with any third party, in accordance with the provisions of this Appendix.

9.2.4 Protected information shall not be saved in a public cloud infrastructure that does not belong to a cloud provider that has won a Nimbus Tender.

9.2.5 The Supplier’s undertakings toward protected information shall remain in effect as long as the information resides in its systems or in the Manufacturer’s systems, even after the end of the Term of the Contract.

9.2.6 The Supplier shall facilitate the retention and full documentation of every access to and use of the various Services by the Customer and its users.

9.2.7 Said documentation shall be retained for a period of at least one year such as to be available to the Customer and the Administrator of the Tender uninterruptedly.

**9.3 Content data**

9.3.1 Customers may generate content data in or by means of the system and may also migrate all content data that they wish to a system in the cloud except where prohibited from so doing by the provisions of law; within this generality, content data may be of different levels of sensitivity, including content data of Customers to which various restrictions apply by force of law, and the Supplier shall neither have any claim against nor impose any restriction thereon.

9.3.2 Israeli laws that apply to some Customers’ content data, as are updated from time to time, impose requirements relating to the protection of information against corruption, modification, or unauthorized exposure. Among other things, said laws that apply to information include the Regulation of Security in Public Entities Law, 5758-1998; the Commercial Torts Law, 5759-1999; the State Property Law, 5711-1951; and specific statutes that pertain to activity of the state and of civil servants in various domains. The obligations relating to information protected under any law are imposed only on Customers that own the information and not on the Supplier, unless explicitly stated otherwise in the Tender Documents. It is the Supplier’s obligation to make every reasonable effort to enable Customers and the Administrator of the Tender to honor the various obligations that devolve upon them under any law in regard to protected information as aforesaid. The contents of this Section shall not derogate from any lawful obligation that belongs to the Supplier.

**9.4 Use of information**

9.4.1 The Administrator of the Tender and the Customers are the sole owners of the information; the Supplier is a processor of the information and shall take no action with respect to it, including saving and storing, processing, and sharing with any third party, except in accordance with the provisions of applicable law in the State of Israel and in accordance with the following:

9.4.1.1 Content data—with the Customer’s authorization by digital instruction and for the purpose of sound delivery of the procured Services.

9.4.1.2 Processing data—at the minimal level needed for sound delivery of the procured Services within the framework of the Agreement, including improving the cyber protection of the Supplier’s systems or services, charging for them, and fulfilling the Supplier’s obligations under the Agreement. It is stated for emphasis that the use of processing data to improve services of the Supplier that are not part of improving said Services for the Customers, among others, is prohibited except when approved in writing by the Administrator of the Tender.

9.4.1.3 Access data—at the minimum level required for sound delivery of the Services procured under the Agreement, charging for them, and fulfilling the Supplier’s obligations under the Agreement.

9.4.2 Without derogating from the aforesaid and to eliminate doubt, the Supplier shall not sell, let out, or take any other commercial action with protected information, including sharing of information after processing, sharing or selling it as part of other uses’ information after deleting identifying details, or under any other circumstances, without the prior written approval of the Administrator of the Tender.

9.4.3 Protected information shall not be saved in the systems of the Supplier or the Manufacturer except in a manner that comports with the provisions of the Agreement and this Appendix and that comports with a digital instruction, and shall ensure the proper removal of said information that resides in its systems, in accordance with the provisions of the law.

9.4.4 Without derogating from the Supplier’s obligations, the Supplier shall take such precautions as are required to ensure that access to protected information is given solely to parties that are authorized by the Supplier and that need access to said information in order to deliver the Services to the Customers. The Supplier shall ensure that the exposure and use of protected information to authorized parties shall be held to the minimum extent needed for the sound delivery of the Service and for compliance with the Supplier’s obligations. The Supplier shall instruct authorized parties in the purposes of the use of the information and the obligations that they must satisfy under law and under the provisions of this Agreement as a result of exposure of the information.

**9.5 Deletion of protected information**

9.5.1 Within 30 days of the day of a request by a Customer or within 90 days of the end of the Contract, for any reason whatsoever, the Supplier shall transfer to the Customer all Customer information unless the Customer states that it has no interest in the information. Insofar as the Service allows a Customer to retrieve or delete information directly, the Supplier shall allow the Customer to take such action up to 30 days after the end of the Contract, provide reasonable assistance for the retrieval or deletion of the information, and present the Customer with proof that all the information has been retrieved or deleted as required. All said information shall be retrieved in a standard, up-to-date, and non-proprietary format.

9.5.2 After 90 days from the end of the Contract or in accordance with a digital instruction to delete information and in accordance with the terms of the Service, all copies of content data in the system or in the environment of the Services shall be fully deleted in a manner that obviates all possibility of their restoration, unless otherwise noted in this Agreement.

9.5.3 Pursuant to the foregoing and in accordance with its lawful obligations, all processing and subscription data that are not needed for the performance of the permissible actions specified in this Section shall be deleted from all records and databases.

**9.6 Confidentiality**

9.6.1 The parties agree that the protected information is confidential and shall not be used in contravention of the provisions of the Agreement or shared with any other party without the prior written approval of the Administrator of the Tender.

9.6.2 The Supplier undertakes to maintain the confidentiality of security tools, including encryption tools, such as encryption stamps and keys, that it makes available to the Customer and [undertakes] not to share with any party technological tools or systems for the decryption of security tools without the prior written approval of the Administrator of the Tender.

9.6.3 Without derogating from the foregoing, the Supplier shall take all requisite actions to maintain the confidentiality of subscription and processing data that are kept in its systems in a confidential and secured manner; within this generality, the Supplier undertakes:

9.6.3.1 that these data shall be protected by means of state-of-the-art technological measures;

9.6.3.2 that access to these data by the Supplier’s employees shall take place only by authorized persons who are required for this purpose and only to the minimum extent necessary.

9.6.4 The Supplier undertakes to ensure that subprocessors acting on its behalf will receive from it access to protected information in order to provide Customers with the Services; they shall be obliged to confidentiality as specified in this Appendix; and, in any case, [the Supplier] shall be held fully responsible for any violation of this undertaking on their part.

**9.7 Israeli service**

9.7.1 All content data shall be kept within the confines of the State of Israel unless otherwise specified within the framework of this Agreement.

9.7.2 Content material within the confines of the State of Israel shall not be exported to any location outside said confines for any purpose including processing, storage, backup, or sharing with a third party in the absence of a digital instruction from the Customer or the prior written approval of the Administrator of the Tender and under such conditions as the Administrator shall specify.

9.7.3 If the Supplier removes protected information from the confines of the State of Israel, it shall delete the protected information immediately and, insofar as this is done for the delivery of Services in accordance with a digital instruction, immediately upon the completion of the operation, in accordance with the terms of the digital instruction and under the provisions of the law.

9.7.4 In any case, a Supplier shall not keep protected information in a country that does not maintain diplomatic relations with the State of Israel.

9.7.5 The contents of this Section shall apply to Service that operates in an Overseas Region, with the necessary adjustments*.*

**9.8 Privacy**

9.8.1 Without derogating from its obligations in the Appendix and the Agreement, the Supplier undertakes to act in accordance with the provisions of the Protection of Privacy Law, 5741-1981 (hereinafter: **“the Protection of Privacy Law”**), its regulations, and any other legislation in accordance with Israel law that regulates privacy in accordance with Israeli law, in order to allow Customers to upload to the cloud private information that is protected under the relevant legislation (hereinafter: **“Private Information”**). It is stated for emphasis in this context that various Customers possess different and varied types of protected information at different levels of sensitivity, such as “medical information” as this term is defined in the Patient’s Rights Law, 5756-1996, personal information, and so on.

9.8.2 The Supplier shall attach an appendix to the Service Agreement containing a detailed account of compliance with the obligations that devolve upon the Supplier under the Protection of Privacy Law and its regulations (hereinafter: **“the Privacy Appendix”**).

9.8.3 The provisions of the Privacy Appendix shall uphold, at the very least, the Supplier’s obligations under this Agreement and Appendix. The Administrator of the Tender may instruct the Supplier to adjust the Privacy Appendix in order to align it with the provisions of the law, the Agreement, and this Appendix.

9.8.4 The Supplier shall update the Privacy Appendix in accordance with changes in the law applying in Israel in regard to Private Information in Customers’ possession, such as to enable the Customers to keep Private Information in the cloud throughout the term of the Contract.

9.8.5 For Israeli service, the Supplier shall not remove private information from the confines of the state of Israel except per digital instruction from the Customer or within the prior written approval of the Administrator of the Tender and under conditions that the administrator shall lay down.

9.8.6 For non-Israeli service, the Supplier shall not remove private information from a region within the confines of the European Union, and the rules of the General Data Protection Regulation (GDPR) shall apply thereto.

9.8.7 Without derogating from the Supplier’s obligations, the Supplier shall keep protected information, such as processing data or subscription data, under its technical control in accordance with the provisions of the law and, particularly, under the Protection of Privacy Law and its regulations.

**9.9 Criminal prohibition against revealing protected information**

9.9.1 Exposure or disclosure of confidential information under this Agreement, be it by commission or by omission, that does not accord with the explicit written consent of the Administrator of the Tender, is a breach of the Supplier’s confidentiality commitment under this Agreement and a criminal offense under Section 118 of the Penal Law, 5737-1977.

9.9.2 In addition and in accordance with the type of information revealed, disclosure of protected information, be it by commission or by omission, in contravention of the provisions of this Agreement or of the law, may be a criminal offense under Israel law in accordance with the type of information exposed (such as Private Information, information classified under Israel law, information that may harm state security, and so on).

**9.10 Applicable law and jurisdiction over protected information**

9.10.1 **Without derogating from the contents of Section 18 of the Contract Agreement:**

9.10.1.1 The State of Israel has a full and exclusive sovereign interest in, and full proprietary powers and prerogatives over, the protected information. Thus, the law that shall apply to protected information is the law of the State of Israel, and the courts of law of the State of Israel shall have sole jurisdiction in any question or proceeding that pertains to said information, with neither restrictions nor exceptions.

9.10.1.2 In any direct dispute between the Supplier and the Administrator of the Tender concerning protected information, the applicable law shall be Israel law and the courts of law of the State of Israel shall have sole jurisdiction in any question or proceeding that pertains to said information, with neither restrictions nor exceptions.

9.10.2 The Supplier shall serve immediate notice of changes or updates in the legal situation that pertains to it that affects the fulfillment of the obligations and rights in regard to protected information under this Agreement. To eliminate doubt, said change shall not have the effect of absolving the Supplier of its obligations under the provisions of the Agreement.

**9.11 Unlawful sharing of information**

9.11.1 Notwithstanding the contents of Section 9.10.1 above*,* if an order is received from a foreign entity concerning the need to obtain, delete, revise, or prevent access to protected information, and if the Supplier believes said request or order is legally binding upon it, whether the information is within the confines of the State of Israel or not, the Supplier shall act in the following manner:

9.11.1.1 It shall promptly apprise the Administrator of the Tender and the relevant Customer of the request or the order and shall inform them of measures that it has taken up to the stage in question, unless explicitly enjoined by law against doing so.

9.11.1.2 Insofar as the request for the information is itself declared classified, [the Supplier] shall act to lift the order and create the possibility of apprising the Administrator of the Tender of the existence of the request.

9.11.1.3 [The Supplier] shall refuse to share the information and shall present all relevant legal arguments, including that the information belongs to a sovereign state and is also under state immunity.

9.11.1.4 To the extent necessary, [the Supplier] shall appeal the decision to the judicial body or the relevant administrative authority and until all possible appeal instances are exhausted and shall request delay of implementation until a final decision in the matter is rendered.

9.11.1.5 In accordance with a request from the Administrator of the Tender, [the Supplier] shall apply to add the Government of Israel as a party to the relevant proceeding.

9.11.1.6 [The Supplier] shall limit the extent of the information disclosed to information that is relevant to the request.

9.11.1.7 [The Supplier] shall demand that the request or the order be honored in accordance with international Mutual Legal Assistance Treaties and shall not comply with the request or order unless this is allowed by the law of the locality where the protected information is situated.

9.11.2 In addition to the foregoing, insofar as a request or order from a foreign entity to receive protected information situated in the State of Israel is made and, in the Supplier’s opinion, said order is legally binding upon it, the Supplier shall do the following in addition to the contents of Section 9.11.1 above:

9.11.2.1 The Supplier shall act in accordance with the provisions of Israel law for the enforcement of the order (such as under the Foreign Judgments Enforcement Law, 5718-1958; the Mutual Legal Assistance Treaties Law, 5758-1998, and so on).

9.11.2.2 In any case, the Supplier shall not enforce an order issued by an organization in a foreign country concerning protected information of the Government of Israel that is situated within the territory of the State of Israel, unless Israeli law so allows.

9.11.3 Without derogating from the Supplier’s obligations anywhere else, the contents of this Section shall apply to the Supplier even insofar as the request from the foreign entity is received by a subprocessor or subcontractor that the Supplier operates for the delivery of the services by force of this Agreement, and that possesses the protected information. In such cases, the Supplier shall step into the shoes of its processor or subcontractor and shall act in accordance with these obligations.

9.11.4 Insofar as the Supplier has reason to believe that it is about to receive a request or an order as aforesaid in Sections 9.10.1–9.11.1 above*,* it shall immediately apprise the Administrator of the Tender of this unless it is enjoined against doing so by law.

**9.12 Requisite actions in cases of sharing of protected information**

9.12.1 Without derogating from the Supplier’s lawful responsibility and without limiting its obligations under this Agreement, in any case where the Supplier has shared protected information with a third party that is not authorized to receive it under the rules of the Tender for any reason whatsoever, including as a result of a request or an order from a foreign authority, the Supplier shall act as follows:

9.12.1.1 The Supplier shall apprise the Administrator of the Tender, immediately and with all possible speed, of any protected information that it has shared as aforesaid, its extent, the recipient’s identity, its reasons for sharing the information, and whether the information was encrypted or protected with additional security tools, and any other relevant information, unless the Supplier is enjoined against doing so by law.

9.12.1.2 The Supplier shall take no action whatsoever that may help to decrypt or remove any technological blockage from protected information in any way and manner whatsoever, be it by commission or by omission. If a law enforcement or defense authority of a foreign country asks to decrypt protected information or make it accessible, the Supplier shall ask the Administrator of the Tender for permission to provide said assistance and shall act in accordance with the Administrator’s instructions.

9.12.1.3 If the protected information has been handed over and the Administrator of the Tender has not been informed (whether due to an order preventing disclosure of the demand to transfer information, whether the demand was made by a defense authority, or for any other reason), the Supplier shall pay the Administrator of the Tender special compensation in the sum of NIS 7,555 within 24 hours from the time the information is handed over.

9.12.2 The content of this Section shall not have the effect of derogating from the Supplier’s responsibility and its undertaking by law and under the provisions of the Agreement not to share protected information without the prior written consent of the Administrator of the Tender, and shall not have the effect of derogating from any right to compensation, indemnification, or any other remedy that the Administrator of the Tender possesses as specified in the Agreement.

**9.13 Supplier’s commitment to information security and cyber security**

9.13.1 The Supplier shall be solely responsible for securing the systems on which the services that it offers Customers are based, be this directly, by a subprocessor, or by means of an agreement concluded in coordination with the provider of the cloud on which the service operates. [The Supplier] shall attend to the regular operation and updating of the security measures and shall ascertain that the technological devices used to secure the information are state-of-the-art and compliant with the highest accepted standard in the market.

9.13.2 The Supplier is responsible for protecting its systems, including dedicated infrastructures, and for the services that it offers against cyber threats and attacks and against any attempt to damage or block access to said infrastructures. Within this framework, the Supplier shall monitor its systems, act to detect and deal with weaknesses in the systems, and update its systems against security exposures with all possible speed, and shall implement mitigation processes insofar as said systems cannot be updated immediately.

9.13.3 The Supplier shall assign a representative who shall be responsible for inquiries about information and cyber security and protection, performance of audits, furnishing of proof as required by the Agreement, alerts against threats, and coping with incidents in real time. Insofar as the service provider operates a Security Operations Center (SOC) to cope with cyber threats, said representative shall share the contact details of this center with the Administrator of the Tender.

9.13.4 The Supplier’s responsibility for information security and cyber protection shall be manifested, among other things*,* in compliance with the following principles insofar as they are relevant for the delivery of the Services:

|  |  |
| --- | --- |
| 1. **Personnel management and training**—ensuring that employees and contractors’ employees acknowledge and understand their responsibilities in the field of information-security policy and cyber protection. | 2. **Supply chain and supplier management**—defining and maintaining mechanisms for management of the entire supply chain of the cloud provider in order to ensure reliability of the infrastructures on which the Services are delivered. |
| 3. **Resource management**—maintaining mechanisms for identification and protection of organizational and information assets, including those of tenants and the Customer. | 4. **Management of actual and suspected security incidents**—having measures in place for management, response, and information-sharing regarding security incidents. |
| 5. **Management of ID and access authorizations**—having mechanisms in place that verify that access to protected information, information-processing resources, facilities, and virtual environments is limited to authorized users only. | 6. **Functional continuity and recovery**—ensuring functional continuity of cloud services, including recovery from disaster while ensuring information reliability and credibility at all times. |
| **7. Encryption and key management**—maintaining secure activity of the Supplier’s services by defining and implementing adequate cryptographic mechanisms. | 1. **Existence of security-level assessment mechanisms**—setting upand managing appropriate testing processes for key components of the network and of information systems that support cloud services, and establishing and managing an appropriate process for assessing the level of protection of critical assets. |
| 1. **Physical and environmental security**—takingpreventivemeasures against unauthorized access to physical sites in order to prevent damage, loss, degradation, malfunction, or theft of organizational assets that may impair the Supplier’s activity. | 1. **Protection of migratability and interoperability**—allocating resources to tenants in order to allow secure interfacing with other cloud services or migration to suppliers of similar services. |
| 1. **Maintenance of secured functional operational continuity**—ensuring secure and sound operation ofthe Supplier’s cyber protection array so that cloud services remain operational at all times. | 1. **Protection of system integrity and reliability**—setting up and taking appropriate measures to assure that the system maintains an adequate level of protection and reliability throughout the life cycle from development to operational deployment, including internal and external development, using commercial and open-code tools. |
| 1. **Communication security**—ensuring digital communication security. | 1. **Risk management**—allocating requisite resources for governance and management of information risks and mechanisms for detection of risks to cloud-service protection. |
| 1. **Protection of personal information**—allocating and managing resources needed to enable Customers to honor their obligation to protect information under their control. | 1. **Adequate cyber protection assessment proceedings**—setting up and taking adequate measures to test security-control proceedings of core cloud-infrastructure systems and networks. |
| 1. **Configuration and modification management**—setting up and implementing modification-management mechanisms for network and information systems. | 1. **Secured development**—allocatingand managing appropriate resources to ensure that the entire life cycle of system development is carried out using secured development methods such as SDLC. |

**9.14 Cyber protection and risk management procedures**

9.14.1 The Supplier shall have cyber-security procedures in place that comport with its undertaking to ensure information security and cyber protection as specified above and to cope with attribution events and threats to cloud infrastructures and Services delivered on their basis (hereinafter: **“the Supplier’s cyber policy”**).

9.14.2 The Supplier shall, on a regular basis, apply risk-management procedures in accordance with the requirements of the standards with which it complies and the requirements of the laws and regulations that apply to it.

**9.15 Standards**

9.15.1 Accepted international standards constitute a basic minimal framework for the cyber-protection infrastructure that the Supplier must maintain. The Supplier shall comply with accepted international standards in the Services that it delivers.

9.15.2 Without derogating from the foregoing, Israeli services shall comply at least with the standards with which the Supplier complies in the Overseas Region. Insofar as the relevant standard certification cannot be obtained in Israel, the Supplier shall fully comply with the requirements of the standard even without obtaining official certification.

9.15.3 At the request of the Administrator of the Tender, the Supplier shall present official certifications of its compliance with the requisite standards. Wherever official certification cannot be obtained, the Supplier shall present the process of control that it performs to comply with the relevant standards and, if asked to do so by the Administrator of the Tender, shall present certifications from an independent outside player that has relevant training and an accepted methodology.

9.15.4 Insofar as said standards are updated or issued in a new version, the Supplier shall update them accordingly.

9.15.5 The Supplier shall publicly update the standards for which the Service has been certified.

**9.16 Regular updates and information sharing in the domain of cyber threats**

9.16.1 The Supplier shall cooperate with the Administrator of the Tender regarding protection against cyber threats as part of the delivery of the Services, in accordance with the following:

9.16.1.1 The Administrator of the Tender shall transfer, subject to the limitations that apply to it and to the policy on information sharing that shall be formulated, information that has the effect of contributing to information security and cyber protection in accordance with the provisions of the Agreement, and, within this generality, information about cyber threats, methods, patterns of attack, and technologies that may be directed against Customers or the Supplier in connection with the delivery of the Services to the Customers.

9.16.1.2 The Supplier shall share with all possible speed, subject to the limitations applying to it and in accordance with the law, information in its possession in order to help Customers and the Administrator of the Tender attend to information security and cyber protection in accordance with the provisions of the Agreement, and, within this generality, information about cyber threats, methods, patterns of attack, and technologies that endanger protected information and the Services that Customers procure.

**9.17 Regular updates and information sharing in the cyber-threat domain**

9.17.1 The Supplier shall allow the Administrator of the Tender and the Customers to use its investigative and IR (incident response) services, insofar as the Supplier offers such services, to cope with security incidents and mishaps or to research and investigate these incidents. Insofar as the Supplier does not have a dedicated IR team, it shall help the Customer to cope with the incident by means of the company’s engineering team or outside players that it operates.

9.17.2 The Supplier shall apprise Customers, in real time if possible, of security incidents and, within this generality, cyber attack and attempted cyber attack against the Customer’s systems and the Supplier’s infrastructures on which the Customers’ systems and data are run.

**9.18 Reliability of employees and suppliers**

9.18.1 The Supplier shall apply accepted processes for review of the reliability of its employees, subcontractors, and suppliers and shall implement a program for detection of and response to security threats of internal origin.

9.18.2 **Subprocessors**

9.18.2.1 The Supplier may honor its obligations under the Agreement by means of subprocessors. All obligations incumbent on the Supplier by force of the Agreement, including this Appendix, shall apply fully to approved subprocessors. The Supplier shall be held fully responsible for any breach of its obligations by means of a subprocessor.

9.18.3 **Instructions for use of a subprocessor**

9.18.3.1 The Supplier shall limit the subprocessor’s ability to access tenant information to the minimum necessary for the delivery of Service or the continued delivery of Service to Customers or end users. The Supplier shall deny to the subprocessor access to information for any other purpose.

9.18.3.2 The subprocessor and all players that it allows to access protected information shall sign a confidentiality commitment and shall honor the confidentiality commitments that apply to the Supplier.

9.18.3.3 The subprocessor shall comply with the undertaking specified in Section 9.4.4 above*,* which states that access to protected information shall be allowed only to personnel who need it and only to an appropriate extent of exposure.

9.18.3.4 It is not against the law (such as privacy law, and so on) to forward information to a subprocessor.

9.18.3.5 The Supplier shall carry out periodic audits of subcontractors that deliver services to Customers.

**9.19 Information security in the Services**

9.19.1 The Supplier shall ensure that the protection and reliability of the Services it delivers shall be on a high level and shall be updated and upgraded throughout the term of the Contract. The Supplier shall not downgrade the level of protection of the services without serving the Administrator of the Tender with prior notice to this effect.

9.19.2 All approved Services shall comply with information- and cyber-security standards that are relevant and accepted in the market. The Administrator of the Tender may ask for certifications of compliance of a given Service with said standards, and in Services that do not yet comply with an official standard, the Supplier shall present a detailed account of the internal checks and third-party laboratories through which the level of the Service was tested, including the testers’ methodologies and certifications. The Administrator of the Tender shall update its cyber policy regarding the approved Services on the basis of proof that the Supplier shall share, among other things.

9.19.3 The Supplier shall have no access to any revision, replacement, or view of information about the Customer’s encryption keys, if any, and shall not put them to any use without the prior written approval of the Administrator of the Tender.

9.19.4 The Supplier shall not deny the Customer the ability to make any use of cyber-protection tools and resources as are needed to secure the Services, including encryption mechanisms that it implements, insofar as this does not impair the sound delivery of the Service.

9.19.4.1 **Periodic audits**

9.19.4.1.1 Once each period, in accordance with the Supplier’s risk management practices or in response to a request from the Administrator of the Tender and in coordination with the Supplier, the Supplier shall conduct an external audit performed by a leading independent company that specializes in such tests (hereinafter: **“the auditing company”**) in order to ensure that the Supplier is complying with the provisions of the Tender or, alternatively, shall allow the Administrator of the Tender to conduct such an audit. The Administrator of the Tender may demand an external audit once per year at the most unless a security incident is being dealt with. The Supplier shall discuss the audit reports that are presented to it at the end of the audit and shall consider the need to update the security procedure following their receipt.

9.19.4.1.2 In the event that the Administrator of the Tender so requests and gives the Supplier advance notice, an auditing company to be approved by the Administrator of the Tender shall perform a special audit in view of a security incident or changes in the Supplier’s security procedures and methods.

9.19.4.1.4 In the event that the Administrator of the Tender so requests, the Supplier shall present the Administrator with an abridged description of the audit findings and the status of their handling.

9.19.4.1.5 The Supplier shall bear the cost of said audits.

9.19.4.2 **Security and intrusion checks**

9.19.4.2.1 The Administrator of the Tender may carry out a check of the implementation of the policy that it specifies for the Customers and the manner in which the Supplier’s infrastructures are being implemented.

9.19.4.2.2 Said check shall be carried out at the level of reviewing the definitions and configuration of the systems as specified by the Customer and also by performing resilience checks for **Customers’** **systems** that are operated by the Supplier’s systems and infrastructures.

9.19.4.2.3 To minimize the risks that these checks involve, the resilience checks shall be coordinated in advance with the Supplier such that the Supplier shall refrain from obstructing those doing the checking.

**9.20 Cyber attack and security incident**

9.20.1 Whenever a cyber attack or security incident in the Supplier’s systems that may affect Customers is detected, the Supplier shall take the following actions:

9.20.1.1 The Supplier shall inform the Customer and the Administrator of the Tender with all possible speed commensurate with the severity of the incident and, in any case, shall do so within a period of time that shall not exceed 12 hours from the moment the cyber attack incident is detected with certainty, except where a competent judicial body issues an order that prohibits this.

9.20.1.2 The Supplier shall take every requisite measure, commensurate with the circumstances of the matter, to mitigate the effects and minimize the damage of the cyber attack.

9.20.1.3 The Supplier shall apprise the Customer and the Administrator of the Tender of measures that they may take to mitigate the effects and minimize the damage of the security incident.

9.20.1.4 The Supplier shall investigate the attack incident and present its findings to the Customer and the Administrator of the Tender for their inspection. Said investigation shall include information that accords with the accepted rules of information-sharing in the cyber domain.

9.20.2 The Supplier shall serve the Customer and the Administrator of the Tender with regular reports about actions that it monitored as attempted cyber attacks focusing on the Customer’s systems.

9.20.3 The Supplier shall learn from security incidents that occurred and shall consider the need to update its systems, processes, and procedures.

9.20.4 In a case where a system such as SaaS experiences a security incident, the Supplier shall indemnify the Customer or the Administrator of the Tender, under the provisions of Section 9.3 of the Contract Agreement, for every reasonable and documented expense that is incurred for the purpose of investigating, applying, narrowing, delineating, and remediating the impairment of the confidentiality, soundness, and availability of the Customer’s information, including processes of notification and disclosure of the event to the relevant authorities.