National Cyber Directorate

Public Tender no. 1-1.2024

"TAFNIT" (PDNS)

Services for the denial of access to malicious domains and redirection enforcement option

Foreword

The National Cyber Directorate (the "Directorate") is a national and technological agency that is in charge of the protection of the national cyberspace of the State of Israel. The Directorate acts in the national level for the continuous strengthening of the cyber protection level of civil organizations, response and elimination of cyber-attacks and preparations for emergencies.
The National Cyber Directorate is interested in purchasing a Protective DNS (PDNS) service in a cloud environment (SaaS) for the purpose of implementing a protection in the state level in the DNS protocol tier as part of the protection umbrella known by the name of "cyber dome."

The service is intended to increase the strength of the organizations that will use it, and therefore increase the strength of the economy, by implementing safe usage of the internet by the denial of access to malicious domains. The service will allow management of the denial policy in different organizational levels, connectivity with different systems and tools and data sharing (import and export) by reports and machine interfaces (API) with other systems.

It is clarified that the engagement by virtue of the Tender is conditional on the existence of a budget.

In this Tender, words which are in the masculine gender shall be deemed to include the feminine gender, and vice versa. The requirements laid down in this Tender are addressed to men and women.

The following is the structure of the Tender:

Chapter A – Description of the tender procedure

Chapter B – Description of the required services and the technological requirements

Chapter C – The bid booklet that will be submitted by the participants in the Tender

Chapter D – Agreement for the pilot period

Chapter E – Agreement with the winning bidder or bidders in the Tender.

Table of contents

0. Definitions

As used in this Tender, the following terms shall have the respective meanings set forth beside them below

0.1 General terms

1.1.1. **Threshold Conditions** – the requirements defining the minimum for the purpose of proceeding to the evaluation stage of the bids as defined in the Tender documents.

1.1.2. **The Directorate/the Office/the Tender Holder** – the National Cyber Directorate in the Prime Minister's Office.

1.1.3. **The Bidder/the Respondent** – any entity that submitted a bid in the Tender.

1.1.4. **The Vendor/the Winning Bidder** – the Bidder whose bid won the Tender and that signed or that is expected to sign an agreement with the Directorate.

1.1.5. **The Bid for the Tender** – the Bidder's bid in accordance with the requirements laid down in the Tender.

1.1.6. **Protected data** – processing data, subscription data and content data.

1.1.7. **Subscription Data** – any information regarding users and clients that the Vendor is required to use for the purpose of managing access, providing the services or for the performance of debits.

1.1.8. **Processing Data** – any information that was created in the Vendor's systems in the course of or as a result of the processing of the content data (meta-data and logs) and that can be attributed in any manner to the Client, to a group of clients or to the user including – user identification and information (including name, address, billing information, date of birth, email, telephone number), log in and log out times from the system, information regarding the clients, services operated by them, configuration data and files, the actions that were performed in the different systems, information regarding the use, IP addresses that were assigned by the different

service providers (Subscription data); Transactional Data and Traffic Data including geolocation of the source and destination of the data, structure of data, track, communication protocol.

1.1.9. **Content Data** – the digital data, including any information, file, database, software, code, logic, datum, report, mark, text, photo, audio, video, photo etc. in any format that were uploaded, created directly by a user, or following its request in the Vendor's systems, including in third-party services used by the Vendor.

1.1.10. **The Tender Holder** – the National Cyber Directorate.

1.1.11. **The Client** – the National Cyber Directorate and the managed organizations.

1.1.12. **Data processing** – an action or a series of actions that are performed in the data, whether or not with automated measures, such as collection, recording, organization, structuring, storage, transfer, modification or change, retrieval or recovery, usage, encryption, distribution or making available for inspection in any other manner, justification or integration, limitation, erasure or demolition etc.

1.1.13. **Performance Guarantee** – a bank guarantee or a guarantee issued by an insurance company in accordance with the provisions set forth in the Agreement, intended to assure the performance of the undertakings of the Vendor in accordance with the provisions set forth in the Tender, according to its bid as approved by the Tender Committee and in accordance with the Agreement.

1.1.14. **Bid Guarantee** – a bank guarantee or a guarantee issued by an insurance company, in accordance with the terms set forth in the Tender, intended to ensure the performance of the undertaking of the Bidder and the signing of the Agreement by the Winning Bidder.

1.1.15. **Year** – 12 months as of the bid submission deadline. It is clarified that this definition is relevant also with respect to the term "year" referred to in the Threshold Conditions section. In any other place

in the Tender documents, reference to the term "year" is to a calendric year.

1.1.16. **Term of engagement** – a period commencing as of the signing date of the Agreement between the Directorate and the Vendor and expiring on its expiration date, including periods in which the Agreement is extended.

1.1.17. **Regulations** – the Mandatory Tenders Regulations 5753-1993.

1.2. Professional terms

1.2.1. **DGA (Domain Generation Algorithm)** – an algorithm that is detected in different families of malware groups that are used for the cyclical generation of numerous domain names that can be used as meeting points with their control and command servers.

1.2.2. **Response Policy Zone/RPZ** – a mechanism for entry of customized policy in DNS servers, in such manner that Translation requests will receive different results from the original/planned translation. The policy can be based on a Block List/Allow List, threat intelligence and more. It is possible to block the access to the proper host/site by changing the result.

1.2.3. **Global Load Balancing Service (GLBS)/Geographic DNS (GeoDNS)/Global Server Load Balancing (GSLB)** – a smart distribution of traffic over server resources located in a number of geographic locations. The servers can be located in the premises of the company itself, or host in a private or a public cloud.

1.2.4. **Managed Organization** – an organization that uses the service within the framework of this Tender, transfers to the National Cyber Directorate data created in the service (service data – telemetry and other data) and operation data, as described in this Tender, and that accepts basic policy for operation from the National Cyber Directorate.

1.2.5. **Betrayal by trusted server** – a DNS server that operates irregularly as a result of a bug or as a result of intentional tampering.

1.2.6. **Response Rate Limiting – RRL** – the ability to limit the number of responses that the DNS server will send to each single client and/or for the specific record. The ability to view the pattern, rate, and signature of DNS queries (Translation requests) more than the queries themselves, as basis for defining the response rate limit.

1.2.7. **Authenticated Denial of Domain Names** – identification of downloading of Resource Records from the translation of a query that was validated and that causes a malfunction in the performance of a scheduled action and that might harm normal usage and/or traffic.

1.2.8. **Interception to normal translation and data flow (Packet Interception)** – tracking queries (by man-in-the-middle eavesdropping) together with forging of response to requests that override the original response as a response to the service translation server PDNS (resolver).

1.2.9. **DNS Poisoning** – the transfer of incorrect data of names of servers and IP addresses linked to them to the DNS system or to its cache memory. This causes to the referral of the request to an address different than the source, as a result of the return of an IP address that is not associated to the original server. This is a category of attacks that includes different attacks such as name chaining, that allows attackers to refer the request to an address following their request.

1.2.10. **DNS Fast Flux** – a change of the DNS records in particularly high frequency for the purpose of helping the attacker conceal the attack.

1.2.11. **DNS Hijacking/DNS Redirection – the registration of a legal domain name with fake data/and/or translation of queries** – incorrect usage for the purpose of redirecting users in the service

unexpectedly to malicious websites (applied in phishing attacks, in the distribution of malware etc.).

1.2.12. **ID Guessing and Query Prediction** – generation of identifiers as id and proper protocol data for the query and its translation by attackers, based on traffic analysis for the purpose of predicting identifiers for a future query and translate it as they wish.

1.2.13. **DNS Foot printing** – a technique for the collection of DNS data regarding the attacked system, that includes domain names, IP addresses and names of computers.

1.2.14. **Price list** – the price list in U.S. dollar and the available pricing models for each catalogue of the services and for all support services, all expert services and any other service that includes human involvement in all available service levels, and that are offered for the use and the consumption of the tenants of the public cloud of the Vendor. It is clarified that the price list is the manufacturer's price list in the country where the manufacturer headquarters are situated. To the extent that the country where the manufacturer's headquarters are situated is the United States, the manufacturer's price list will be the price list of the State of Washington D.C.

1.2.15. **DNS Tunneling/Covert Channel** – transfer of concealed data by a DNS protocol.

1.2.16. **Domain Name System** – a protocol allowing access in such manner that the end units in the internet will be able to translate domain names that are more convenient for natural human use (website URL) to the actual numeric addresses (IP addresses) to which they will direct during the communication while using a translating server (DNS Resolver).

1.2.17. **Passive DNS domain names system** – a collection of DNS data that were translated, and that allows saving of history thereby identifying efficiently malicious websites and domain names.

1.2.18. **DNS Amplification attack** – an amplification attack of a system of domain names (DNS) is one of the many types of distributed denial-of-service attacks (DDoS). Same as in any DDoS attack, the purpose of the attackers is to deny from users access to the system, service, internet websites, application, or any other resource by slowing down the response or causing complete shutdown. While most of the DDoS attacks operate by flooding a system with an immense amount of average-size packets, an amplification of a DNS attack uses larger data units for the purpose of accomplishing the same outcome.

1.2.19. **Reflection Attack** – users in a number of primary serves of a DNS zone that store the final versions of all records in the same zone – for the purpose of attacking one entity. The attack is performed by sending fake queries as a target to the primary servers for the purpose of creating responses in a rate that might be bigger in scope than it was possible in a generic DDoS attack of the type amplification attack.

1.2.20. **Spoofing** – a type of fraud in which an attacker impersonates as another by forging data such as email, text message, website URL or other for the purpose of impersonating before a specific target to convince it that it maintains an interaction with a recognized and reliable source.

1.2.21. **DDoS Attack/Flood Attack** – an attack in which attackers send a very high volume of traffic to the system in such manner that the system does not have enough time to analyze and enable permitted traffic network or deny prohibited traffic. There are a number of types of DDoS attacks, such as an attack on non-existing servers (NXDOMAIN Attack) – in which the attacker floods the DNS server with a large volume of requests for queries that do not exist or that are illegal, amplification attack, reflection attack.

1.2.22. **Service User** – any use of the service within the framework of the National Cyber Directorate and/or the organizations that use the service within the framework of this Tender.

1.2.23. **Abuse of wildcards in domain names** – an attack that disrupts the ability to identify in a reliable manner the source of the query and the accuracy of the information when using wildcards in domain names.

1.2.24. **Endpoint IP** – an IP address to which a device can connect and be used by the user while using the internet.

1.2.25. **Service Data** – data created during the service in the course of its operation and that are used as detection and identification data (D&I).

1.2.26. **Deny List/Block List** – a list containing names of domains and sub-domains to which access is denied.

1.2.27. **Allow List** – a list containing names of domains and sub-domains to which access is permitted.

1.2.28. **Protective DNS Service (PDNS)** – a service analyzing queries/requests for translation (DNS queries) and that takes action for the purpose of handling threats while using the existing DNS protocol and architecture. The service denies access to malware, ransomware, phishing, viruses, spyware, and access and/or use of communication and/or malicious websites.

1.2.29. **Guiding service/directory service** – a software product used for the storage, distribution, and search of shared information in a computer network. The major information categories that are managed by the software include users, email addresses or telephone numbers, folders, files, printers, passwords of computer users, permissions, configurations of distributed applications, public keys and more.

1.2.30. **Service provided in the Israeli region or Israeli service** – a service that is included in the manufacturer's price list and that is fully provided from the Israeli region, when the entire processing, data traffic and saving of the content data are performed in the Israeli region only.

1.2.31. **International Domain Name/IDN** – an internet domain name that includes at least one of the following: a symbol, a letter in an alphabet other than English (for example Cyrillic, Chinese, Arabic, Hebrew and more), special characters (as customary in French for example). These domain names are stored in the domain names system (DNS) as an ASCII string by Punycode syntax.

1.2.32. **Orphan DNS server** – a DNS server with a registered address in DNS despite the fact that the domain in which it is located has no DNS records by itself and therefore it does not exist.

* References to the allow/block lists of domain names (domains/sub-domains) in this Tender also include the option for blocking or permission of the IP addresses.

Chapter A – Description of the Tender procedure

1. Presentation of the Tender

1.1. Subject matter of the Tender

The National Cyber Directorate is interested to purchase a Protective DNS service (PDNS) in cloud configuration (SaaS) that will constitute a component in the protection umbrella for the interface known by the name of "cyber dome" and that will allow protection in a state level in the DNS protocol layer.

The purpose of the service is to increase the strength of the economy by denying access to malicious domains for the safe use of the internet and, in certain cases, also for the purpose of denying access to specific types of services.

The service will make available the data to the user by a portal, by way of pull and push, and in different resolutions, and will allow to export the information that it collects manually, as a report, or automatically, by a machine interface (API) to other systems. The service requires a management interface that will allow the management of the service in a hierarchical manner to a number of organizations, and a local management interface for the purpose of managing the service for a group of organizations or for a single organization.

Within the framework of this Tender, the National Cyber Directorate plans to operate the service internally (a description that is part the requirements is provided further below) and allow to organizations and users in the market to operate this service, in the level of the different sectors, critical State infrastructures and more. The National Cyber Directorate will operate the service in the Directorate itself and will monitor the operations of the service within the framework of the work of the relevant users on behalf of the Directorate (the Defense Division and the Technology Division)

This Tender is intended to provide a service that will protect the economy for a number of years and for many organizations.

Each user and/or organization will be able to operate the service independently and directly (including a registration for the service) and will

receive the regular integration and support services directly from the winning bidder(s) as stated in this Tender. The National Cyber Directorate will be able to operate the service for the Directorate itself and manage, on a general level, the service for specific groups of organizations, in different aspects (for example, basic policy that is required for protection) concurrently with the current operation of the organizations for themselves, during the period that the service is provided in accordance with this Tender.

It is clarified that the engagement by virtue of the Tender is conditional on the existence of a budgetary source.

1.2. Tender stages

1.2.1. **Inspection of compliance with the Threshold Conditions** – at this stage the Tender Holder will inspect whether the bids comply with the Tender Threshold Conditions. Bidders whose bids comply with the Threshold Conditions will undergo a security check by the security division in the Directorate. Bidders whose identities are approved by the security division in the Directorate will proceed to the stage of evaluation of the bid as stated hereunder.

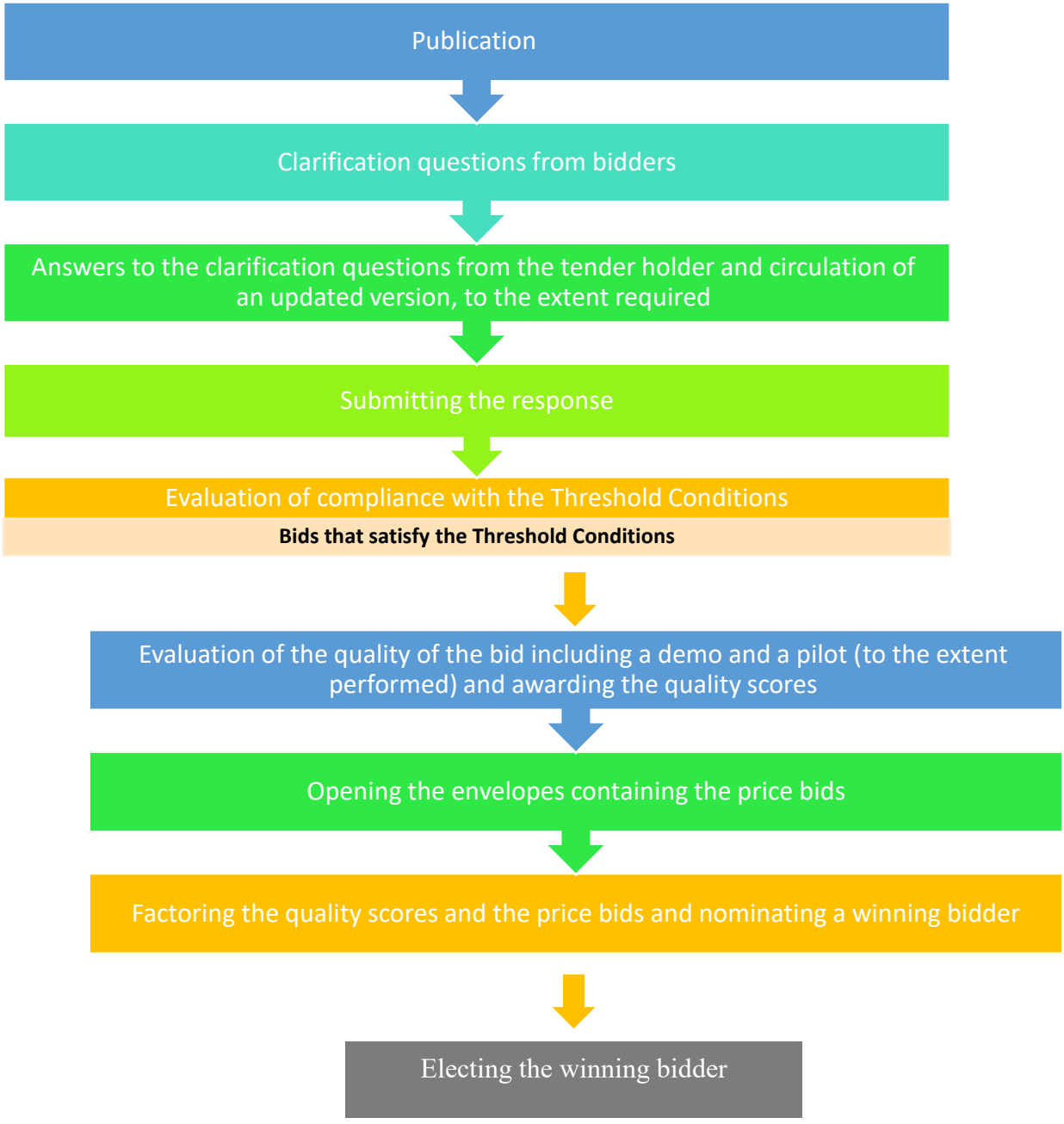
1.2.2. **Evaluation of the quality of the bids** – after receiving the bids of the bidders who passed the Threshold Conditions stage, the Tender Holder will award quality score to each bid according to the parameters described in the Tender, and that include a demonstration (demo) and a pilot of the solution that is proposed to the Directorate. After completing the evaluation and the scoring of the bids, the quality scores for each bid will be awarded. It is clarified that the pilot stage is optional and subject to the decision of the Directorate.

1.2.3. **Evaluation of the price bids** – after awarding the quality scores, the envelopes containing the price bids of all bidders who complied with the minimum Threshold Conditions will be opened, and the price scores for each bid will be set.

1.2.4. **Final score** – weighting the quality score together with the price score.

1.2.5. **Election of a winning bidder** – at this stage the Directorate will consider whether to engage with the winning bidder – who was awarded the highest final score, and, in addition, whether to engage with the next-ranked bidders.

1.3 Diagram of the Tender stages



2. Phases and dates in the Tender

2.1. Submission of bids in the Tender

2.1.1. Bids in the Tender will be submitted based on the following schedule:

Activity	Date	Time
Date of distribution of the Tender to the list of bidders	28.1.2024	12:00
Bidders' conference	20.2.2024	TBA
Deadline for delivery of the clarification questions by the bidders	5.3.2024	12:00
The date the Directorate delivers its answers to the clarification questions	22.3.2024	16:00
Deadline for submission of the bids in the tender box	14.4.2024	12:00
Effect of the bid and effect of the guarantee in respect of the bid until	14.8.2024	

2.1.2. In the event of a conflict or discrepancy between the dates as stated above and other dates as stated in the Tender, the dates set out in the table above shall take precedence.

2.1.3. The submission of a bid means that the Bidder declares that it satisfies the Threshold Conditions of the Tender in general, understands the essence of the services subject matter of the Tender, agrees to the entire terms of the Tender and that prior to the submission of its bid it received the entire possible information, inspected the data, particulars and the facts and therefore the Bidder shall be precluded from raising any claim that it did not know and/or did not understand any detail and/or any condition in the Tender including all particulars and parts thereof.

2.1.4. The bid in the Tender will be submitted in the tender box no later than the dates and the times as stated in the table of dates presented in section 2.1.1 above. The tender box is situated in 10 HaBarzel St., bldg. C, Ramat HaChayal Tel Aviv, fl. 4.

2.1.5. Bids that will not be submitted in the tender box until the bid submission deadline as stated in the table of dates will be disqualified in limine.

2.2. Bidders' conference

2.2.1. A bidders' conference will be held in the offices of the National Cyber Directorate in Tel Aviv on the date set out in the table of dates as stated in section 2.1.1 above. An exact location will be provided shortly before the date of the conference.

2.2.2. A Bidder who wishes to participate in the bidders' conference is requested to notify the Tender Holder regarding its participation in advance by email to the email as stated in section 2.3.

2.2.3. Bidders are required to deliver to the Tender Holder, in 24 hours at the latest prior to the date of the bidders' conference, the name of the Bidder and the full information of the representatives on behalf of the Bidder who are expected to attend the conference.

2.2.4. Participation in the conference is recommended and does not constitute part of the Threshold Conditions for the submission of a bid in the Tender.

2.2.5. Answers that are provided in the bidders' conference will bind the Tender Holder only if given in writing and in accordance with the instructions set forth in section 2.3.

2.3. Clarification questions regarding the Tender

2.3.1. Ms. Miriam Davidov, the Procurement Field Director in the National Cyber Directorate, is the representative on behalf of the Tender Holder who is in charge of this Tender.

2.3.2. Any queries in connection with this Tender shall be referred to Mr. Miriam Davidov and shall be made in writing only by email: **cyber-michrazim@cyber.gov.il**.

2.3.3. Any queries and clarification questions will include the Tender name and number, the name of the inquiring company, the name of the inquirer, address and email and telephone number.

2.3.4. The questions of the Bidders shall be delivered by email to the contact person whose information is provided in section 2.3.2 above. The Bidder is responsible for confirming over the phone that its entire questions reached the contact person.

2.3.5. The questions of the Bidders will be submitted both in PDF format and in an Excel file in the following format:

Serial no.	Section in the Tender or in the contract	The question

2.3.6. Bidders are required to assure that the PDF file and the Excel file will include questions in identical wording and order. In any event, the PDF file shall be deemed as the binding version.

To the extent that there are a number of questions regarding a specific section, it is necessary to write the section and any question referring to that section in a separate line.

2.3.7. To the extent that until the deadline for the submission of questions the Bidder delivers its questions to the Tender Holder a number of times, the Bidder is required to add in each query the new questions to the file of the previous questions that the Bidder delivered, cumulatively. The only file with questions that the Tender Holder will respond to will be the last file that the Tender Holder received on the deadline for the submission of the clarification questions as stated in the table of dates, as stated in section 2.1.1 above.

2.3.8. The Directorate will not be required to answer questions that will be delivered after the said date or that will be referred verbally or over the phone or in another format than required.

2.3.9. The Directorate shall be entitled to allow other rounds of clarification questions, at its discretion.

2.3.10. Any queries concerning clarification questions and requests shall be made in Hebrew or English only.

2.3.11. The answers of the Tender Holder to the questions that were submitted will be published in the Tender page in the internet website of the Government Procurement Administration in the link provided above and by the Directorate internet website. It is clarified that the Bidder is fully and exclusively responsible for receiving updates to the answers of the Tender Holder and regular updates regarding this Tender that will be published as said.

2.3.12. Only answers that were published in the manner as stated above shall bind the Tender Holder and shall constitute an integral part of the Tender. For the avoidance of doubt, verbal answers shall not bind the Tender Holder unless published and distributed in writing to all Bidders in accordance with the provisions of section 2.3.11 above. The Tender Holder is not bound by the wording of the question and in this regard the Tender Holder shall be entitled, while drafting the answers of the clarification questions that will be sent to the Bidders, to shorten the wording of a question or rephrase such question. Without derogating from the foregoing, the Bidder is responsible for wording the questions in a manner that will not include identifying information about the Bidder or about any other entity.

2.3.13. Bidders are responsible for raising any question or doubts that the Bidders have in connection with any contradiction or non-conformity between the different Tender documents or between different instructions in the same document, during the stage of the clarification questions. It is clarified that if no clarification question is asked on a particular question prior to the submission of the bid, then, to the extent that any discrepancies or non-conformances are found afterwards as said, and these cannot be resolved, the Tender Holder shall interpret these discrepancies and its interpretation shall bind the Bidder. Bidders are required to take into consideration the fact that such contradictions shall be interpreted in a manner that broadens the obligations of the Bidder or the rights of the Tender Holder or the Client.

2.3.14. The Tender Holder shall be entitled to make any change in the Tender documents and ascribe an interpretation or a clarification to the provisions set forth in the Tender documents, also following its own initiative and irrespective to the questions made by the Bidders.

2.4. Answers by the Directorate to the clarification questions

2.4.1. The answers that the Directorate will give to the clarification questions will be in Hebrew and/or English only, at its sole discretion.

2.4.2. The answers to the clarification questions will be published in the internet website of the Government Procurement Administration. It is clarified that the answers of the Directorate to the clarification questions will be worded in a manner that does not disclose the identity of the inquirers.

2.4.3. In the answers to the clarification questions the Directorate shall be entitled to make any change in the Tender documents, and interpret or clarify the instructions set forth in the Tender documents.

2.4.4. The Directorate is not bound by the wording of a question that was submitted, and in this regard the Directorate shall be entitled, when drafting the answers to the clarification questions that will be sent to the Bidders, to shorten the wording of a question or rephrase a question. The wording decided by the Directorate is the binding wording and constitutes an integral part of the Tender.

2.4.5. It is emphasized that when submitting a bid, the Bidder is required to submit as part of its bid the document of questions and answers that is relevant to that stage, signed by the Bidder. The signed Q&A document shall constitute part of the Tender documents and in the event of discrepancy between the Tender documents and the Q&A document – the Q&A document shall take precedence.

3. The Tender procedure

3.1. Authorities of the Directorate when holding the Tender procedure and evaluating the bids

3.1.1. The Tender documents will be published in Hebrew, and the Directorate will publish by their side a proposed translation to English. For the avoidance of doubt, the Tender procedure will be held in Hebrew and the binding version will be the version published in Hebrew. The Directorate reserves the right to contact Bidders and/or publish clarifications also in English, at its sole discretion. In the event of discrepancy between the Hebrew version and its translation – the Hebrew version shall take precedence.

3.1.2. The Directorate or a team on its behalf that might also include external consultants will evaluate the bids submitted in the Tender. For the purpose of evaluating the bids, the Directorate or anyone acting on its behalf will use the professional knowledge in its possession and reliable information sources, including public information about the Bidder, the opinion of professional consultants and any other reliable source of information.

3.1.3. The Directorate or anyone acting on its behalf shall be entitled to request from a Bidder to explain certain details in its bid, complete deficient information in its bid or provide another or alternative document proving its compliance with the Tender terms and conditions, and the Tender Threshold Conditions, within a specific period of time. Failure to respond to such a request as said or failure to deliver an answer not within the period of time that was defined might result in the disqualification of the bid.

3.1.4. After the Bidder was afforded an opportunity to complete and amend its bid, the Directorate shall be entitled to disqualify a bid that still fails to satisfy the requirements laid down in the Tender or, at its discretion, request additional information.

3.1.5. Review of the bid guarantee

3.1.5.1. The bid guarantee shall be an unconditional and autonomous guarantee, payable on demand made solely by the Directorate, and the Directorate shall not be required to give reasons for its decision.

3.1.5.2. The guarantee shall be a digital guarantee from a bank or an insurance company in accordance with the provisions set forth in Financial and Economic Regulations (TAKAM) Directive no. 7.3.3 – Guarantees, and TAKAM Directive 14.4.1 – Digital guarantees.

3.1.5.3. The Bidder shall solely incur the expenses in connection with the issuance of the bid guarantee.

3.1.5.4. The bid guarantee will be used as a security ensuring the compliance of the Bidder with its undertakings within the framework of this Tender and the signing of the Agreement (chapter E of the Tender documents) by the winning bidder. In the event that the Bidder withdraws from its bid and/or fails to perform any of its undertakings under this Tender, the Directorate shall be entitled to forfeit the bid guarantee, as pre-estimated liquidated damages, without derogating from the right of the Directorate to claim any additional relief and/or damages under any law.

3.1.5.5. The bid guarantee shall constitute an integral part of the bid and shall be submitted jointly with the bid. In the event that the Tender Committee concludes that the bid guarantee fails to satisfy the terms of the guarantee set out above, the Tender Committee shall be entitled to disqualify the Bidder's bid.

3.1.5.6. Without derogating from the rights of the Directorate, any deviation from the wording of the guarantee set out in Appendix 10 shall not give rise to grounds for disqualification of the bid, provided that the bid

guarantee that was submitted satisfies, in the manner prescribed by the Tender Committee, the conditions set out in section 3.1.5. The Tender Committee shall be entitled to permit to a Bidder to make immaterial amendments in the bid guarantee in 7 days as of the date the Tender Committee made its announcement, provided that the Tender Committee did not conclude that the defects in the bid guarantee are material defects, defects that were caused in bad faith or as a result of manipulation or an intention to maintain an improper leeway.

3.1.6. Material defects in the bid guarantee for the purpose of this matter shall be deemed as the following defects:

3.1.6.1. A guarantee that did not specify the guarantee amount as stated in section 4.1.8.

3.1.6.2. A guarantee that was not in effect at least until the date set out in section 2.1.1 (including).

3.1.6.3. A guarantee that is not provided for the Bidder's bid or a guarantee that fails to satisfy the conditions regarding its unconditional and autonomous status, and that is payable following a unilateral demand made by the Directorate and without giving reasons for its decision.

3.1.6.4. The guarantee that is not issued by an authorized entity, as stated above.

3.1.6.5. The Directorate shall be entitled to demand from the Bidders to extend the effect of the bid guarantee for a period of up to 90 additional days, by delivery of written notice to the Bidders. In such circumstances as said Bidders shall submit a new bid guarantee (or will extend the effect of the original bid guarantee that they provided) in seven days as of the date of receiving the notice from the Directorate.

3.1.6.6. If the winning bidder in the Tender was announced, the effect of its guarantee shall be extended according to the instructions of the Directorate. After the winning bidder signed the Agreement, provided certificates of insurance and the bid guarantee as said in section 6.4 hereunder.

3.1.6.7. If the Bidder did not win the Tender, or in the event that the bid was disqualified by the Directorate, or in the event of cancellation of the Tender, and without derogating from any other right of the Directorate, the bid guarantee shall be returned to the Bidder in 60 days as of the date the Directorate made its decision for the purpose of this matter.

3.1.6.8. Early evaluation of the bid guarantee: Bidders shall be entitled to submit for the approval of the Tender Committee the wording of the bid guarantee that the Bidders intend to submit, until the deadline for the delivery of the clarification questions, as stated in section 2.1.1 in the Tender documents. The Tender Committee shall be entitled to approve this wording or give comments on this wording, and publish the approved wording, including permitted amendments, and any other of its responses on the subject to all Bidders, while omitting the identity of the Bidder that submitted the bid guarantee as said. The aforesaid shall be without prejudice to the liability of the Bidders for the full and complete guarantee that will be submitted and it is clarified that the Bidder shall have no claim or demand against the Tender Committee in the event that the Tender Committee disqualified a bid guarantee that was approved earlier, provided that the disqualification is in compliance with the provisions of the law and case law.

3.1.7. The Directorate shall be entitled to disqualify a bid as a result of lack of detailed response to any of the sections in the Tender and/or an ambiguous and unclear bid that, in the opinion of the

Directorate, prevents a proper evaluation of the bid. In addition, the Directorate shall be entitled to disqualify a bid that disregards or stipulates on the requirements laid down in the Tender, qualifies its provisions, alters the wording of the sections in the Tender or Appendixes thereof, or that is not in conformance, in any other manner, to the requirements laid down in the Tender.

3.1.8. The Directorate shall be entitled not to accept the cheapest bid or any bid in whole or in part, at its sole discretion.

3.1.9. Submission of improved price bids:

3.1.9.1. After opening the price bids, the Directorate shall be entitled, however not obligated, to allow to Bidders who were awarded the minimum quality score to submit an improved bid. The number of the submission rounds of the improved price bids shall be decided at the sole discretion of the Directorate. At the end of each round a Bidder shall be entitled, however not obligated, to submit to the Directorate an improved final bid, with relation to its previous bid. In the event that a single bid is left, the Directorate shall be entitled, at its sole discretion, to allow the said Bidder to submit an improved bid.

3.1.9.2. In the event that an improved bid was submitted, the price score will be calculated again based on the amended price bid that was submitted.

3.1.10. After the election of the winning bidder in the Tender, the Tender Committee shall be entitled to apply to the winning bidder and request to improve its bid.

3.1.11. The Directorate shall be entitled to accept only part of the bid, and not the entire bid, at its sole discretion.

3.1.12. Without derogating from the other provisions set forth in the other sections in the Tender, the Directorate shall be entitled to disqualify

a bid at its sole discretion, if one of the following conditions is satisfied:

3.1.12.1. **Disqualification of an unprofitable bid or a manipulative bid** – if the bid is unprofitable to the Bidder to the extent that it questions its ability to perform its undertakings if it wins the Tender, or if the bid is a manipulative bid (for example, a bid that includes extraordinary prices or discounts for certain items) both with relation to the bid itself and with relation to other bids, and in any event of bad faith action.

3.1.12.2. **Disqualification on the grounds of bad faith conduct in previous tenders** – the Bidder, within the framework of a previous tender held by the Client, or by another entity, conducted with cunning, manipulation or lack of clean hands, or provided misleading or inaccurate material information.

3.1.12.3. **Disqualification of the bid on the grounds of the financial position of the Bidder** – if, as a result of its present or expected financial position of the Bidder, including as a result of bankruptcy or liquidation proceedings or material claims held against it, there is a concern regarding the performance of the Bidder if the Bidder wins the Tender.

3.1.12.4. **Disqualification on the grounds of a conflict of interests** – if there is a conflict of interests, whether direct or indirect, or a concern about a conflict of interests between the interests of the Bidder or its interested parties, and the performance of the services by the Bidder in a manner that cannot be resolved, in the opinion of the Directorate.

3.1.13. Upon the occurrence of the events enumerated in sub-sections 3.1.12, the Bidder shall have a right to present its case in writing or

verbally, prior to the delivery of the final decision, subject to the discretion of the Directorate.

3.2. Cancellation or modification of the Tender

3.2.1. The Directorate shall be entitled, following its initiative and at its discretion, to cancel the Tender, modify and update the Tender, and in this regard update the dates set out in the Tender, make changes in the Agreement and in the other Tender documents, shorten, cancel, or change the demo process. Such changes as said will be published in the website of the Government Procurement Administration (it is necessary to type in the search line the reference number: 4000582798).

3.2.2. In any event of performance of changes that affect the pricing of the bids or that have a material effect on the essence of the services that are included in the Tender, the Bidders shall have the option to withdraw or amend their bid.

3.2.3. The engagement with the winning bidder in the Tender is conditional on the existence of available budget. To the extent that for budgetary reasons it will be impossible to engage with the winning bidder in the Tender, or in the event it will be necessary to reduce the scope of works, the Directorate shall be entitled to cancel the Tender or reduce its scope or delay the relevant dates.

3.2.4. The Directorate shall not be obligated to compensate the Bidders in the event of cancellation, reduction, or delay of the Tender.

3.3. Bids of Bidders that currently provide a service to the Directorate

Within the framework of its activities, the Directorate maintains at present and/or maintained in the past engagements with companies that provide and/or that provided services to the Directorate also in fields that are relevant to the services that are required in this Tender ("Similar Engagements"). The Directorate shall be entitled, at its sole discretion, to allow to the companies with which the Directorate maintains and/or maintained Similar Engagements to submit a bid in this Tender according to the Tender rules. The mere supply of a service within the framework

of Similar Engagements shall not constitute an advantage to the Bidder or prevent from the Bidder to submit a bid in this Tender. To the extent that the bids are submitted, the bids will be evaluated in accordance with the rules of this Tender, same as any other bid that will be submitted within the framework of the Tender.

3.4 Expenses

The Bidder shall not be entitled to reimbursement of expenses or to any compensation in connection with the Tender, including in the event of discontinuation, delay, change of terms or cancellation of the Tender.

3.5 Jurisdiction

The competent courts in the place of residence of the Tender Committee of the Directorate shall have sole jurisdiction in anything relating to and arising out of this Tender or any suit stemming from the Tender procedure. The Tender shall be governed by the laws of the State of Israel.

3.6 Ownership of the bid and the use of the bid

This Tender is the intellectual property of the Directorate and is delivered to the Bidders solely for the purpose of submitting the bid. The Tender may not be used for any purpose other than for the purpose of preparing the Bidder's bid in this Tender.

3.7 Confidentiality of the bid and right of inspection

3.7.1. The Directorate undertakes not to disclose the content of the bid that will be submitted in this Tender to a third party other than the employees of the Office or consultants employed by the Office for the purpose of the Tender, who shall also be bound by the duty of confidentiality and no use of the Bidder's bid however solely for the purpose of the Tender.

3.7.2. Nevertheless, it is clarified that pursuant to Regulation 21(e) of the Mandatory Tender Regulations, Bidders who did not win the Tender shall be entitled to request an inspection of the winning bid, and other documents that are related to the Tender. The Directorate

shall deny from Bidders to inspect the bid documents or other documents that are related to the Tender in respect of which the Tender Committee on behalf of the Directorate decided that they include a trade secret or a professional secret, or might harm the security of the State, its foreign relations, its economy, and the security of the public, and all in accordance with the provisions set forth in the Regulations.

3.7.3. If a Bidder wishes to deny inspection in other sections of its bid on the grounds of trade secret, professional secret or any other reason as stated in the Mandatory Tender Regulations, the Bidder shall specify this expressly in the bid booklet. It is clarified that the mere request shall not deny inspection of the relevant sections, and that the Tender Committee on behalf of the Directorate shall make a decision for the purpose of this matter.

3.7.4. A Bidder who argued that a specific part of its bid is a trade secret or a professional secret shall be precluded from demanding an inspection of this part in the winning bid in the Tender.

3.7.5. In the event that the Tender Committee on behalf of the Directorate dismisses the claim of the winning bidder alleging that parts of its bid are a trade secret or a professional secret, the Tender Committee shall deliver to the Bidder notice for the purpose of this matter at least 5 workdays prior to actually granting the right of inspection.

3.7.6. Subject to the provisions set forth in this section, by participating in the Tender the Bidder agrees that its entire bid, including all Appendixes thereof, shall be made available for the inspection of the other Bidders in the Tender under any law and the Mandatory Tender Regulations.

4. Threshold Conditions for participation in the Tender

Only Bidders who satisfy the following requirements on the bid submission deadline shall proceed the Threshold Conditions. Proof of compliance with the Threshold Conditions as stated hereunder shall be provided in accordance with the instructions set forth in the bid booklet.

4.1. Administrative Threshold Conditions

4.1.1. The Bidder is a corporation lawfully registered in Israel or abroad.

4.1.2. The Bidder does not hold or is not held by another Bidder in the Tender (holding for the purpose of this matter – holding directly or indirectly of 25% or more of the means of control, as meant by this term in the Securities Law 5728-1968) and another entity does not hold 25% or more of two Bidders. In addition, the Bidder is not a subcontractor on behalf of another Bidder in the Tender in connection with the performance of the services in this Tender.

4.1.3. The Bidder keeps books of account and records that the Bidder is obligated to keep in accordance with the provisions of the Income Tax Ordinance [New Version] and the Value Added Tax Law 5736-1975 (hereinafter: the "VAT Law") unless it is exempt from keeping these documents.

4.1.4. The Bidder reports to the Assessing Officer regarding its income and reports to the Director regarding transactions that are chargeable with tax, in accordance with the provisions of the VAT Law.

4.1.5. No convictions: the Bidder and any "interested party" related to the Bidder (as meant by this term in section 2B of the Transactions with Public Bodies Law) were not convicted of more than two offenses in accordance with the provisions of the Foreign Workers Law 5751-1991 and the Minimum Wage Law 5747-1987 or were convicted as said, however at least one year since the date of the last conviction and until the submission date of the bid lapsed.

4.1.6. Proper representation: the Bidder complies with the provisions of section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 or that the provisions of the said law do not apply to the Bidder, and acts in accordance with the provisions set forth in section 2B1 of the Transactions with Public Bodies Law.

4.1.7. **Obligation to engage in industrial cooperation** – the Bidder undertakes to perform all actions that are required for the purpose of maintaining industrial cooperation in accordance with the provisions of Mandatory Tender Regulations (Mandatory Industrial Cooperation) 5767-2007 (hereinafter: the "**Industrial Cooperation Regulations**"), in the event that the provisions of these Regulations apply as part of the competitive procedures that will be conducted by virtue of the Tender.

4.1.8. **The bid guarantee/Tender guarantee**

4.1.8.1. The Bidder is obligated to provide to the tender holder a guarantee for the purpose of performing its bid (hereinafter: the "**Bid Guarantee**") in the amount of ILS 1,500,000 (hereinafter: the "**Guarantee Amount**") in the wording as provided in Appendix 10 of the bid booklet. The bid shall be in effect no later than the bid submission deadline and until the date that was set for the date of effect of the bid and the effect of the Bid Guarantee, as stated in the table of the dates in section 2.1.1, up to and including.

4.2. Professional threshold conditions

4.2.1. The Bidder is the manufacturer of the proposed product/system/service and holds the rights therein.
Alternatively, the Bidder is required to be an authorized reseller on behalf of the manufacturer of the proposed product/system/service.

4.2.2. The service that is proposed within the framework of this Tender shall be a cloud-based service[1].

4.2.3. The Bidder has experience in the last 3 years in the supply of the proposed product/service within the framework of the response to this Tender in the following minimum scopes:

4.2.3.1. The product was supplied/the service was provided to at least 75 organizations (of the governmental or public or private sector).

4.2.3.2. Out of the organizations enumerated in section 4.2.3.1, at least 10 organizations have 5,000 users per organization and at least 1,500 queries per day for each user.

4.2.3.3. Out of the organizations enumerated in section 4.2.3.1, at least 45 organizations have 3,000 users per organization and at least 1,500 queries per day for each user.

4.2.3.4. Out of the organizations enumerated in section 4.2.3.1, 20 organizations have at least 100 users per organization and at least 1,500 queries per day for each user.

4.2.4. For each of the 75 organizations enumerated in section 4.2.3.1, the Bidder performed integration and provided dedicated support by a dedicated team of employees that were trained for the purpose of this matter, over the period of one year as a minimum (in the years 2019-2023).

It is clarified that compliance with this Threshold Condition may also be proven by a vendor/subcontractor with whom the Bidder maintained/maintains a dedicated engagement for the purpose of this matter.

The Bidder is required to state whether the vendor/subcontractor complies with this condition as stated above.

[1] Bidders are required to take account of the fact that the service that is provided should be a cloud-based service (SaaS) according to the government policy as stated in Government Resolution 231 dated August 1, 2021.

4.2.5. The Bidder is required to present experience under the definition/update of the block policy in at least 5 organizations, out of the list of organizations enumerated in sections 4.2.3.2 – 4.2.3.4 that receive the service.
The definition of the block policy shall be manifested also by the fact that the Bidder can incorporate intelligence feeds from different sources and/or in different formats, including the ability to include the information that is provided by an external entity.

4.3. Restructuring in the Bidder

4.3.1. In the event that the Bidder, as a discrete legal entity, fails to satisfy the professional Threshold Conditions set out above, and a restructuring occurred in the Bidder's history (for example, acquisition of activity, incorporation as a company, reorganization or consolidation of companies in another manner) in such manner that the relevant activity for the purpose of satisfying the Threshold Conditions was incorporated in the Bidder; the Bidder may request from the Tender Holder to rely on the experience of the entity wherein the activity was performed prior to the restructuring, for the purpose of satisfying the Threshold Conditions. A decision regarding such recognition as said shall be made subject to the discretion of the Tender Holder.

4.3.2. In such circumstances as said the Bidder shall be obligated to attach to its bid the proper references, including a merger agreement or a part thereof, a resolution of the board of directors and any other document that will satisfy the Tender Holder. A decision regarding such a recognition as said shall be made subject to the discretion of the Tender Holder.

5. Ranking the bids

5.1. Quality Score

5.1.1. Awarding the quality score

5.1.1.1. The Directorate shall award the score for each of the components forming the score of the bids as stated above, according to an internal evaluation criteria document that will be decided prior to the submission date of the bids.

5.1.1.2. The evaluation of the quality score includes three stages, when each stage will be awarded a score and this score will be amended after the evaluation of the next stage, to the extent that the Bidder complied with the minimum requirements for the purpose of proceeding to that stage. Bids that fail to receive the minimum quality score in each stage will be disqualified and will not proceed to the next evaluation stage.

5.1.1.3. **The total minimum quality score in this quality stage is a total score of 75% after the completion of all evaluation stages**. It is clarified that the bids that will not be awarded the minimum quality score at least after the completion of the evaluation of the quality stage will not proceed to the next stage. Accordingly, the envelopes containing the price bid of bids that did not receive the minimum quality score for this stage will not be opened.

5.1.1.4. Stage A: evaluation of the features of the proposed service: at this stage the compliance of the proposed service with the professional requirements laid down in the Tender will be evaluated (Appendix 9 in Chapter C), quality of compliance with the different requirements and compliance of the proposed service with the requirements and specifications of the

Directorate – based on the written bid that was submitted.

5.1.1.5. The minimum quality score at this stage for the purpose of proceeding to the next stage is a total score of 60% of the points from the general calculation of the features of the proposed service and at least 10% of the points in each of the sections that were marked as important ("R").

5.1.1.6. Stage B – the DEMO stage: within the framework of the evaluation of the quality for the purpose of awarding the quality score Bidders will be required to present a demonstration (demo) of the service with relation to the scenarios described in Appendix 9 in Chapter C. For that purpose, the Directorate shall deliver to all the Bidders who satisfied the Threshold Conditions an invitation to a meeting, in which the Directorate will announce the date and time of the meeting, its expected duration, the place and manner of its performance (the meeting will be held from a remote location, by way of VC) and will give highlights regarding the manner of demonstration of the system. The minimum quality score for the purpose of proceeding to the next stage, after completion the evaluation of this stage and after correcting the quality score is 65%.

5.1.1.7. Stage C: the pilot stage, to the extent that the Directorate decides to perform the pilot: compliance with the pilot requirements and compliance with the professional requirements during the performance of the pilot while actually implementing the proposed service by entities in the Directorate, in accordance with the requirements laid down in the Tender, and in accordance with other instructions, to the extent that such instructions are delivered to the Bidders. The minimum quality score for the purpose of proceeding

to the next stage, after completing this stage and correcting the quality score is a score of 75%.

5.2. The pilot stage within the framework of the evaluation of the quality score

5.2.1. General

5.2.1.1. In accordance with the instructions set forth in this Tender, a group of Bidders that satisfied the Threshold Conditions will perform a pilot, during which it will provide the services described further below.

5.2.1.2. The pilot will be an operational pilot, i.e., the use of the service will be full use implemented by different entities in the Directorate, while making ordinary use of the service according to the daily needs and the requirements of the Directorate. The data that will be produced from the performance of the pilot will be used by the Directorate, same as any other data that is produced from systems that the Directorate uses – i.e., the pilot will examine the usability of the system under an operational scenario by the Directorate teams, including the use of the data for the purpose of sending notifications together with data from other information sources in the Directorate.

5.2.1.3. The pilot will continue up to 45 days as of the date of its commencement, as stated in the Agreement, for the pilot period (**Chapter D** of the Tender).

5.2.1.4. The Directorate shall be entitled to shorten the period of performance of the pilot, in the event that the Directorate finds, at its sole discretion, that there is no point in continuing the performance of the pilot with a Bidder (for example: fast success or, alternatively, no material success) or in the event there is an operational

need or any other need that requires to shorten the period.

5.2.1.5. The Directorate shall be entitled to cancel completely the pilot stage, at its sole discretion.

5.2.1.6. The pilot shall be performed in return for no payment. Prior to the commencement of the pilot, the Bidder will be required to sign the Agreement for the pilot period (**Chapter D** of the Tender), that includes information regarding the conditions and the maintenance of performance of the pilot. Signing the Agreement by the Bidder and the Directorate is a condition for the performance of the pilot. The appendixes specified in the pilot agreement shall be attached thereto.

5.2.1.7. To the extent that a Bidder provides a service to the Directorate as stated in section 3.3 of the Tender documents, the pilot shall be performed in accordance with the conditions in the transfer and the Agreement for the pilot period (**Chapter D** of the Tender) irrespective of the existing service that will continue according to the terms applicable thereto. Accordingly, the Bidder shall be obligated to provide to the Directorate user licenses and service licenses for the pilot period, in accordance with the Agreement for the pilot period, concurrently with the continuation of the performance of the existing service.

5.2.1.8. By its agreement to perform the pilot, each Bidder agrees to the decision of the Directorate to conduct the pilot and receive the instructions of the Directorate for the purpose of conducting the pilot, and the manner of scoring the pilot, as stated in section 5.2.3 hereunder.

5.2.2. **Framework for the pilot**

5.2.2.1. For the purpose of performing the pilot, the vendor is required to provide to the Directorate 6 licenses under

different profiles for the full use in the system. In addition, the vendor is required to make available to the Directorate at least one managed organizations' manager license as a minimum.

5.2.2.2. Prior to the commencement of the pilot the vendor shall provide training regarding the use of the system to the pilot users on behalf of the Directorate. The training shall be provided by a video conference on the date set by the Directorate for the purpose of this matter.

5.2.2.3. The use of the system during the pilot period shall be made according to the scenarios that were described in Appendix 9 of Chapter C.

5.2.2.4. The Bidder is required to make available to the pilot users the full support services as stated in Appendix 9 in Chapter C.

5.2.3. **Scoring the pilot quality**

5.2.3.1. Prior to the commencement of the pilot, the Directorate shall define the indicators for the purpose of determining the pilot success.

5.2.3.2. After the end of the pilot period, the Directorate will award a quality score to the pilot based on the indicators that were defined in advance, and that will include, *inter alia*, reference to the following indicators: usability (interface, convenience of use etc.), conformance to the Bidder's bid in the Tender as submitted, quality of the data and the deliverables produced from the use of the proposed service according to the usage scenarios, level of conformance to the Directorate requirements, level of support and training of the Bidder.

5.2.3.3. The minimum quality score that is required for the pilot is a total pilot quality score of 65 as a minimum. Bids that are not awarded the minimum quality score for the

pilot will not proceed to the stage of election of the winning bidder and awarding of the final score.

5.3. Discount percentage

5.3.1. Subject to the provisions set forth in this section, the discount that is proposed within the framework of the price bid will be valid during the entire term of the Agreement for all services, as stated in this Tender. If the catalogue of the services offers the service under different pricing methods, the discount shall apply to all.

5.3.2. This discount shall be added to the discounts that are already part of the manufacturer's price list (such as bulk discount, commitment-based pricing etc.).

5.3.3. The vendor shall be entitled to increase its discount for the term of the engagement. This change will be permanent as of the date of setting the new discount percentage and until the end of the engagement, except for circumstances in which the vendor requests to increase its discount again.

5.3.4. Without derogating from the foregoing, the discount that is proposed in each of the groups of discounts will change in the following manner during the term of engagement:

5.3.4.1. Bracket A – when the scope of consumption of all clients of a specific service exceeds USD 620,000 cumulatively during a calendric year, the discount percentage in each discount group as said will increase by 5 percentage points over the proposal that the vendor makes in its bid (for example, of the bid presents a discount of 55% the new bracket will be 60%).

5.3.4.2. Bracket B – when the scope of consumption of all clients of a specific service exceeds USD 2,100,000 cumulatively over a calendric year, the discount percentage in all discount groups as said will increase by 5 percentage points over the previous bracket.

5.3.5. If the discount for a specific service was updated based on the brackets defined above, however at the end of a calendric year the scope of procurement from a specific service dropped below the brackets set out above, the vendor shall be entitled to contact the Tender Holder for the purpose of updating the discount back to the previous bracket with relation to the bracket wherein the vendor is in, for the next calendric year.

5.4. Price list for the proposed services

5.4.1. Overseas price list and Israel price list

5.4.1.1. The overseas price list and the Israel price list shall be as defined above.

5.4.1.2. The Bidder is required to attach a link to the overseas price list of the service, according to its definition above, and mark it as Appendix 14 in Chapter C. If the overseas price list is not public, it is necessary to attach it as an appendix to the bid. In such circumstances as said, the rules set out in section 5.4.1.3 hereunder shall apply to the said price list.

5.4.1.3. Price lists that are not public should be signed by an official representative on behalf of the manager who is responsible for the said territory, or by its superior or by officers in the management of the manufacturer. With regard to the price list for a third-party service, the said price list will be signed by an official representative on behalf of the third-party manufacturer who is responsible for the said region or by its superior or by an officer in the management of the manufacturer. For the avoidance of doubt, the Tender Holder reserves the right to demand additional/other approvals, including a demand for the signature of another representative on behalf of the manager for the official price list.

5.4.2. **<u>The determining price list</u>**

5.4.2.1. A price list for services that are provided in an overseas region – the dating price list will be the overseas price list.

5.4.2.2. The price list for services that are provided in the Israel region

5.4.2.2.1. The determining price list will be the price list based on which the clients will purchase services in the Israeli region and from which the discounts that the Bidder offers for these services will stem. The determining price list will be set in accordance with the following instructions:

5.4.2.2.2. The lowest price for each service out of the following price lists:

5.4.2.2.3. <u>Overseas price list</u> of the service in the services catalogue of this region.

5.4.2.2.4. <u>Israel price list</u> for the service in the services catalogue of the Israeli region in the manner set out by the Bidder for the customers in the territory and that is published in public.

5.4.2.2.5. A change in an overseas price list – the following arrangements shall apply in the event of an extreme change in the price of an overseas price list as a result of exogenous changes over which the vendor has no control, and that do not exist in the Israeli region:

5.4.2.2.6. The vendor may request from the Tender Holder to change the overseas region to another region that is in the EU and that is one of the 3 regions with the highest volume of sales in the EU, and will give reasons for its request.

5.4.2.2.7. The Tender Holder shall review the request positively and to the extent that the said request does not affect the clients in an unfair manner, it will approve the request.

5.4.2.2.8. To the extent that the Tender Holder approved the change of the overseas region, the prices of the former overseas region will be used as the maximum prices in the new overseas region.

5.4.2.2.9. The Bidder undertakes to allow the Tender Holder to have free, full and independent access to the full price list for all the public regions from which the clients can order the services, as of the submission date of the bids and during the entire term of engagement.

5.4.3. **Price of the services for a client by virtue of this Tender will be set in accordance with the following provisions**

5.4.3.1. The price of the services in the overseas region will be the overseas price list of the service, as of the date of consumption of the service, minus the percentage of discount that was offered by the vendor for that service.

5.4.3.2. The price of the services in the Israeli territory will be the overseas price list of the service as of the date of consumption of the service, minus the percentage of discount that was offered by the vendor for that service or the price list price of the service in the Israeli region, as of the date of consumption of the service, minus the percentage of discount that was offered by the vendor for the same service, whichever is lower.

5.4.4. **PS hours and integration hours**

5.4.4.1. The Bidder is required to take into consideration that within the framework of the services that the Bidder

will provide as part of this Tender the services will include PS hours and integration hours in estimated scopes and for the following rates.

5.4.4.2. The required scope of hours for the term of engagement:

Item	Quantity in the first year of engagement	Quantity in the second year of engagement	Quantity in the third year of engagement
PS hours	200	100	100
Integration hours	200	100	100

It is clarified that the scope of the hours is estimated and that the Directorate is under no obligation to purchase any minimum number of hours.

5.4.4.3. Hourly rate:

Item	Rate per hour	Rate per hour (excluding VAT) in the second and third year of engagement
PS hour	770	690
Integration hour	785	705

5.4.5. **Price updates**

5.4.5.1. If the manufacturer's price list was updated, the vendor shall be entitled to update the price lists during the term of the engagement for the purpose of making such an update as said, and the price lists in their latest version shall be delivered to the Tender Holder, and the Tender Holder shall review the updated price lists and their conformance to the requirements laid down in the Tender, and update the prices of the services that were approved for purchase accordingly. The vendor shall be responsible for delivering the updated price lists.

5.4.5.2. From the time the vendor delivered to the Tender Holder a complete request for a price update, according to the requirements made by the Tender Holder, the Tender Holder shall update the clients regarding the updated prices within a period of time that will not exceed 30 workdays.

5.4.5.3. The price updates shall enter into force as of the date the clients received a notice in connection therewith, and shall not apply retroactively.

5.5. The price bid/price of the bid

5.5.1. At the time of submitting the bid in this Tender, the Bidders shall provide a price bid that will be submitted together with the bid in a sealed and separate envelope on which the number of the Tender will be written, including the words "price bid" and the Bidder's name. The submission shall be made in accordance with the provisions of Appendix 8 in chapter C.

5.5.2. **Structure of the price bid**

5.5.2.1. The following are the components of the price bid:

A= fixed monthly cost for management and maintenance of service – the cost refers to all inputs that the Bidder is required to invest in the performance of the services by virtue of this Tender, except for a direct cost of licensing. The cost includes inputs including; manpower, setup and operation, customer service etc.

B= fixed discount (in percentage) from the official price list of the manufacturer.

5.5.2.2. A weighted price for the Bidder shall be calculated for each bid that complied with the requirements laid down in the Tender and in the minimum quality threshold

defined in section 5.1 above, based on the following formula:

$$Pi = A*36 + (1-B)*P*X*4$$

5.5.2.2.1. **P** is the price for an annual license of use as stated in the official price list prices of the manufacturer.

5.5.2.2.2. **X** is an estimate of the required number of annual licenses. This quantity is multiplied by 4 for the purpose of summarizing the annual number of licenses for a period of 5 years estimated for full deployment in the span of 3 years.

5.6. Manner of weighting the bid and ranking of Bidders

Bids shall be ranked based on the following mechanism:

5.6.1. The quality score, as defined in each bid, as stated in section 5.1, will be marked as Qi.

5.6.2. The price of the bid, as calculated for each bid, as stated in section 5.5.2, will be marked as Pi.

5.6.3. The average price of the three bids with a quality score ranging from 80 to 100 will be marked as $\hat{P}$. In the event that there are no three bids that satisfy the criterion, $\hat{P}$ shall be set as the average of the 3 bids estimated by the Tender Holder for the Tender price.

5.6.4. Calculation of the bid score:

The score of the Bidder's bid shall be set by calculating the "estimated price" (EP), this price will be set according to the following formula:

$$EP(P_i, Q_i) = \begin{cases} P_i - 0.005 * (Q_i - 90) * \widehat{P} & 90 \le Q_i \le 100 \\ P_i - 0.03 * (Q_i - 90) * \widehat{P} & 80 \le Q_i < 90 \\ P_i - (0.04 * (Q_i - 80) - 0.3) * \widehat{P} & 75 \le Q_i < 80 \\ \infty & Q_i < 75 \end{cases}$$

The lower the EP, the higher the ranking of the bid, when the best bid is the bid with the lowest EP.

5.6.5. The estimate price is a ranking tool only and not the actual price of the bid; payment to the winning bidder shall be made based on its proposal for the bill of quantities.

5.6.6. The Bidder with the lowest EP (with the higher ranking) will be announced as the winning bidder described in section 6 hereunder.

5.6.7. The following is a numeric example:

Weighting the price:

The average of the bids with a score higher than 80 is 553

Bid	Quality score	Price	Estimated price	Ranking
A	90	572	**572.00**	**1**
B	95	598	**584.17**	**4**
C	85	490	**573.00**	**2**
D	78	365	**575.27**	**3**
E	72	360	∞	

- As said, in the first stage the average of the Lessor's Works with a quality score of 80-100 is calculated. Bids A, B, C satisfy the criteria, and therefore the average between their prices is calculated: (572+598+490)/3=1,660/3=**553.33**.

- For each of the bids, the estimate price for the bid is calculated according to the quality score. For example, for bid C the estimate price will be calculated according to the

second line, because the quality score is 85: 490-0.03*(85-90)*553.33=490-0.03*(-5)*553.33=490+83=**573**.

- For bid B, the estimate price will be calculated according to the first line, because the quality score is 95: 598-0.005*(95-90)*553.33=598-0.005*5*553.33=598-13.83=**584.17**.

- For bid D, the estimate price will be calculated according to the third line, because the quality score is 78: 365-(0.04*(78-80)-0.3)*553.33=365-(0.04*(-2)-0.3)*553.33=365+210.27 =**575.27**.

5.6.8. The price will include all related services that are required under this Tender, including API that is not limited in the number of calls (API calls) and that allows the use of the entire system capabilities, including technical support, operational support, training, SLA, and any other related service that is required for the purpose of receiving the services under the Tender.

5.6.9. For the avoidance of doubt, it is clarified that the Directorate is not obligated to purchase any minimum number of monitored users or organizations.

5.6.10. To the extent that the Bidder offers other off-the-shelf services in addition to the services that are required and as stated in this Tender however that are related to its scopes such as (however not limited to): additional reports, extensions to the proposed system, whether independent and whether by integration with third-party vendors etc., the Bidder may submit a price list that includes the list of the additional services and an explanation specifying the scope of each service. During the term of engagement, the Directorate shall have the option to purchase from the winning bidder additional services that are specified in the price list for a discount of at least 25% of the prices that will be stated in the price list that will be submitted or from the updated price list at the time (whichever is cheaper), including also products and services that constitute an extension to the proposed system by integration with third-party vendors, under the conditions set out in the Agreement.

5.6.11. During the term of engagement, the Directorate shall have the option to pay for the first year of engagement in advance and for two or three years in advance.

6. Election of the winning bidder

6.1. Ranking the bids

6.1.1. The bids shall be ranked based on the ranking awarded to them according to the information provided in section 5.6 above, when the highest-ranked bid will be ranked first, followed by the second-ranked bid and so on and so forth.

6.1.2. At this stage the Committee shall act in accordance with the provisions of section 2B of the Mandatory Tender Law 5752-1992 regarding a "business controlled by a woman" as meant by this term in that section.

6.1.3. In the event that an identical price was calculated for two (or more) bids, the bid with the highest quality score will be ranked first. If the quality score of the bids is identical, the bid with the standard deviation of the quality score components which is the lowest shall be ranked first.

6.2. Election of the winning bidder

6.2.1. Upon completion of the procedures described above, the Tender Committee will announce the election of the Bidder whose bid was ranked first as the winning bidder, subject to the performance of the actions described hereunder, and shall notify the other Bidders regarding its decision as said.

6.2.2. The Tender Committee shall be entitled to elect the Bidder whose bid was ranked second, and afterwards the Bidder whose bid was ranked third and so on and so forth, as second eligible Bidder, third eligible Bidder and so on and so forth (the "Eligible Bidder").

6.2.3. If the winning of a winning bidder in the Tender is canceled for any reason in the period of up to 6 months as of the date of its election as the winning bidder, the Tender Committee shall be entitled to declare the following Eligible Bidder as the winning bidder subject to its compliance with the requirements laid down hereunder.

6.3. Announcing a nominated winning bidder

After completion of the procedures described above, the Tender Holder shall announce the Bidder whose bid was ranked first as the nominated winning bidder (hereinafter: the "**Nominated Winning Bidder**").

6.4. Duties of the Nominated Winning Bidder

6.4.1. The Nominated Winning Bidder shall be obligated to perform the following actions within a period of time that will be defined by the Tender Holder, before it is declared as the winning bidder:

6.4.1.1. The Nominated Winning Bidder shall be required to demonstrate its compliance with the supply chain method of the National Cyber Directorate in accordance with the instructions of the Security Division in the Directorate that will be delivered to it, within a period of time that will be defined by the Tender Holder.

A link containing an explanation regarding the supply chain method is hereby attached (the National Cyber Directorate):

https://www.gov.il/he/departments/guides/supply_chain_guide?chapterIndex=2

The Nominated Winning Bidder shall be required to comply with the required controls (in the modules: system-wide requirements, cloud-based systems, website storage) in the Excel file hereby attached in the following link:

https://www.gov.il/BlobFolder/guide/supply_chain_guide/he/Supplier%20Questionnaire%201.4%20V1.47.xlsx

6.4.1.2. The Nominated Winning Bidder shall submit the Agreement attached in **Chapter E** including all Appendixes thereof, in its latest version, signed by the

authorized signatory on behalf of the Bidder and bearing the stamp of the corporation, and that will include the following:

6.4.1.2.1. Performance guarantee – as stated in **Appendix E** of the Agreement.

6.4.1.2.2. Insurance requirements – as stated in **Appendix F** of the Agreement.

6.4.2. The Tender Holder reserves the right to forfeit the guarantee for the submission of the bids in the Tender, in the event that the Nominated Winning Bidder fails to satisfy the requirements laid down in the Tender; or withdraws from its bid; or fails to sign the Agreement as required; or fails to provide a guarantee as required, or acts in bad faith.

6.4.3. To the extent that the Nominated Winning Bidder fails to satisfy one or more of its obligations as stated above within a period of time that was defined by the Tender Holder, the Tender Holder shall be entitled, at its sole discretion, to grant it an extension to complete the performance of the actions, disqualify its bid, announce the next-ranked Bidder as the Nominated Winning Bidder, and forfeit the Bidder's guarantee.

7. Engagement with the winning bidder

7.1.1. The Directorate shall be entitled to engage with the Bidder who was ranked first in the final score and decide whether to engage also with the next-ranked Bidders.

7.1.2. The Directorate shall be entitled to declare a second-eligible Bidder. The bid of a Bidder who is declared as a second-eligible bidder shall be in effect for a period of XXX.

7.1.3. The Directorate does not undertake to engage with any of the Bidders in the Tender, and it reserves the right, after completion of the Tender, to engage with another entity for the purpose of receiving the services as stated in this Tender, in accordance with the provisions of the Mandatory Tender Regulations.

7.1.4 A Bidder who received notice that the Tender Holder intends to announce it as the winning bidder in the Tender shall be obligated to perform the following actions within the period of time set out by the Directorate:

7.1.4.1 To provide to the Directorate the Agreement for the entire term of the Agreement between the parties, when the Agreement and all Appendixes thereof are signed, including the Appendixes and the sections in the Agreement that refer to the performance guarantee and the Certificate of Insurance, according to the demands made by the Directorate

7.1.4.2 If the Bidder is an Israeli corporation, it is required to register in the suppliers portal, in accordance with the instructions set forth in TAKAM Directive no. 7.12.5, "Suppliers Portal," and perform all actions that are required from the Bidder as stated in this Directive, and in this regard pay for the costs that are required for the purpose of connecting to the portal. Alternatively, if the Bidder uses the suppliers portal,

the Bidder shall provide a confirmation for the purpose of this matter.

7.1.5. Failure to provide the documents that are required as stated in this section on the date set for the purpose of this matter, without obtaining the approval of the Directorate, might result in the cancellation of the winning of the said Bidder.

Chapter B – Description of the required services and the technological requirements

8. General description of the required service

8.1. The National Cyber Directorate is interested to purchase a Protective DNS service (PDNS) in cloud configuration (SaaS) that will constitute a component in the protection umbrella to the economy that is known by the name of "cyber dome."

8.2. The service is a core communication service for its users.

8.3. The purpose of the service is to increase the strength of the economy by denying access to malicious domains by denial of translation (Resolving) to their IP addresses and/or enforcing the redirection to an approved server and/or to a sinkhole server and/or to a block page with a message to the user of the service or lack of translation (NXDOMAIN message) for the safe use of the internet and, in certain cases, also for the purpose of limiting internet usage of specific types of services.

8.4. The protection will focus on different categories such as: malware and the distribution/installation of malicious software, phishing attacks, use of a component in the command infrastructure (C2), use as component of exfiltration infrastructure etc. The service will allow to inspect suspicious domains and make a decision regarding the type of actions concerning the Translation requests relevant to them.

8.5. The service will allow the National Cyber Directorate to optimize the protection of the Israeli economy in the field of safe internet use according to a dynamic policy based on enriched Block Lists by Threat Intelligence, collection of intelligence and feedback of enriched service data (D&I), content screening, detection of anomalies and malware products, detection of data leak by a DNS protocol, support of different types of protocols and more.

8.6. The service will make accessible to the user of the service the management and tracking capabilities of the data according to the information provided in this Tender, by a user interface (Portal/UI).

8.7. The service will have a general management interface that will allow the management of the service in a hierarchical manner for a number of organizations and a local management interface for the purpose of managing the service for a group of organizations or for a single organization.

8.8. The service will allow to export the data that the service collected manually as a report or automatically by a machine interface (API) to other systems.

8.9. The service will be able to connect to the Israeli Internet eXchange that is maintained by the Israel Internet Association and according to the instructions of the Association.

8.10. The service and the data that will be provided by the service will be used by the National Cyber Directorate, together with additional information sources of the Directorate, in response to the improvement of the cyber protection in different fields, according to the requirements of the Directorate and for the purpose of performing its roles.

8.11. The service will be able to operate independently and without interfering in the functionality in the event the State of Israel is disconnected from the worldwide internet network, whether the reason for this stems from a technical malfunction, a cyber incident, or another reason.

8.12. The option for the consumption of the service by the tenants will not be conditional on the performance of installation of a software component (including a virtual appliance) or hardware in the tenant's premises.

9. Term of engagement

9.1. Terms of engagement

9.1.1. The term of engagement under this Agreement is for 3 years as of the date the Tender Holder announces the commencement of the engagement (the "Term of Engagement").

9.1.2. The Directorate shall have the option to expand and/or extend the Term of Engagement by additional periods that will not exceed 7 additional years (a total of up to 10 years as of the signing date of this Agreement) in accordance with the provisions set forth in this Agreement and subject to the provisions set forth in the Mandatory Tender Law.

9.1.3. The option right shall be exercised as long as the Office wishes to continue and receive the services. The Agreement shall be extended based on the provisions set forth in the original agreement, or under conditions that benefit with the Tender Holder as agreed in writing between the parties.

9.1.4. It is clarified that the engagement by virtue of the Tender is conditional on the existence of a budget.

9.1.5. **Organization period**

9.1.5.1. A maximum period of 60 calendric days (up to the first two months as of the period of performance of the service) as of the date the Tender Holder announces the commencement of the engagement. During the organization period, the vendor shall make arrangements for the purpose of providing integration and support services (hereinafter: the "**Integration and Support Services**") as stated in section 11, directly by dedicated employees or by a subcontractor.

9.1.5.2. If the Integration and Support Services are provided directly by the winning bidder, the dedicated integration and support team will include employees

who have extensive knowledge of the service and its features – content experts with experience of at least one year in the operation and support of the service and the proposed dedicated product.

The vendor shall provide employees with a valid security clearance or, alternatively, will act for the purpose of performing a security clearance for them.

9.1.6. **Period of performance of the service**

9.1.6.1. This period shall commence after completion of the organization period to the satisfaction of the Directorate.

9.1.6.2. It is clarified that to the extent that the vendor completes the organization period earlier than the period set out in section 9.1.5 above, the vendor shall commence with the performance of the service according to its definition in this Tender.

10. Involved entities

10.1. Professional supervision

The Tender Holder or anyone acting on its behalf shall be entitled to use the services of professional entities or a consultant who will act as an auditor for the procedure, give answers to professional questions and will act as a professional umpire in the event of a professional dispute.

10.2. Managed organization

An organization that uses the service within the framework of this Tender, and that transfers to the National Cyber Directorate data created in the service (service data – telemetry and additional data) and operation data, as described in this Tender and that receives a basic operation policy from the National Cyber Directorate.

10.3. Team on behalf of the master vendor for the performance of the services

10.3.1. Project Manager

10.3.1.1. After receiving the notice regarding the winning, the vendor shall appoint on its behalf a project manager who will act as the contact person (hereinafter: the "**Project Manager**") with the Tender Holder and who will serve as the contact person in anything related to the performance of the Tender. The Project Manager who was appointed shall be replaced after delivery of written notice to the Tender Holder in connection therewith.

10.3.1.2. The Project Manager shall act as the representative on behalf of the master vendor for all intents and purposes in connection with the performance of the services, and this shall not derogate from the undertakings of the master vendor and from its liability under the Agreement. A request by the master vendor to the Tender Holder shall be made by the Tender Holder. A

query or a notice by the Tender Holder to the Project Manager shall be deemed as a query or a notice to the vendor.

10.3.1.3. The Project Manager shall manage the required activity within the framework of the Tender, coordinate and supervise all entities that are related to the activity and shall fill in its role as stated in the Tender. The Project Manager shall act as a representative on behalf of the winning bidder and its contact person for the purpose of maintaining the regular connection between the Client and the winning bidder, and with respect to any other matter that requires interaction between the parties.

10.3.1.4. The Project Manager shall act for the purpose of achieving optimal and high satisfaction level of the Tender Holder/Client. In this regard, the Project Manager shall act for the purpose of assuring the compliance of the winning bidder with the entire conditions and requirements laid down in the Tender, including the implementation and integration of advanced service levels and strategies.

10.3.1.5. The Project Manager shall be responsible for the direct connection with the representatives on behalf of the Directorate within the framework of this Tender, the management of work processes, the management of updated versions of the service, its development, technological development, upgrade according to the request made by the Directorate and the conduct of the integration and support team.

10.3.1.6. The Project Manager shall be responsible for integration of the inter-organizational activity of the winning bidder that stems from the requirements laid down in the Tender, including a summary of reports and performance and submission status of execution

reports and regular settling of accounts with the Tender Holder/Client.

10.3.1.7. The Project Manager shall be responsible for the current operation of the control, supervision, and command systems such as: process quality control mechanisms, lesson learning and performance of corrective actions in real time in the work of the winning bidder, vis-à-vis the Tender Holder/the Client and its representatives.

10.3.1.8. Reporting to the Tender Holder regarding the status of activity of the winning bidder.

10.3.1.9. The Project Manager shall dedicate the entire time that is required for the purpose of performing all missions and tasks that are required from it within the framework of this Tender, and by the Tender Holder/the Client during the entire Term of Engagement or according to the instructions of the Client, and in any event for a period of time that will not fall below six months as of the commencement of the engagement.

10.3.1.10. **General requirements**

10.3.1.10.1. The vendor undertakes that during the entire Term of Engagement the Project Manager will have Israeli citizenship and his permanent place of residence will be Israel or in another country whose time zone is different by up to two hours (behind or ahead) with relation to the Israeli time zone, and subject to the approval of the Directorate of the country where the Project Manager will stay.

10.3.1.10.2. The vendor shall update the Directorate one month in advance prior to any permanent or temporary replacement of

the Project Manager or his country of residence.

10.3.1.10.3. A vendor whose Project Manager on its behalf fails to comply with the conditions set forth in section 12.1 above shall be obligated to satisfy this demand in one year as of the date of signing the Agreement.

10.3.1.10.4. To the extent that the permanent place of residence of the Project Manager is not Israel, the Project Manager will arrive to Israel for the purpose of providing a service in accordance with this Agreement, following the demand of the Directorate that will be deliver a reasonable time in advance and in reasonable frequency according to the requirements of the Directorate. It is clarified that the vendor shall incur all expenses in connection with the arrival and the stay in Israel.

10.3.1.10.5. The Directorate shall be entitled to demand from the vendor to replace the Project Manager, at any time and without giving reasons for the demand.

10.3.2. **<u>The dedicated integration and support team</u>**

10.3.2.1. The dedicated integration and support team will include the employees on behalf of the Bidder and/or the subcontractor (as stated in the Threshold Conditions), with a high level of knowledge of the service and its features –

10.3.2.1.1. With experience of at least 3 years in the field of data communication.

10.3.2.1.2. With experience of at least 3 years in the world of system, Microsoft environment, Linux and cloud.

10.3.2.1.3. With experience of at least 3 years in the integration of data security solutions.

10.3.2.1.4. With at least one permanent team member who arrives to the National Cyber Directorate and to the managed organizations, who is a content expert and with experience of at least one year in the integration, operation and support of the service in the request subject matter of the service in the Tender (PDNS service).

10.3.2.1.5. Advantage to holders of international certifications in the field of data communication, system, cyber.

10.3.2.2. The team, that will include a sufficient number of members and in any event no less than one team member, will provide current integration and support services including support of the service itself and its management interfaces, as stated in this Tender. The services will be provided to the National Cyber Directorate and to all the managed organizations that receive the service in accordance with this Tender.

10.3.2.3. The team will provide integration services to the National Cyber Directorate and to the managed organizations, and support services, whether physical or from a remote location, according to need and the required response and in coordination with the National Cyber Directorate and the relevant managed organizations.

10.3.2.4. The integration and support team will be required to assist in the performance of supplementary integration tasks in the premises of the different tenants such as the following:

10.3.2.4.1. Installation of Virtual Appliance/Roaming Clients in the tenant.

10.3.2.4.2. Blocking access of the endpoints to the internet by a traditional DNS protocol.

10.3.2.4.3. Blocking access of endpoints to the internet by DoH protocol.

10.3.2.4.4. Blocking access of the endpoints to the internet by DoT protocol.

10.3.2.4.5. Blocking access of the endpoints to traditional and public DNS servers on the internet (such as PUBLIC RESOLVERS etc.).

10.3.2.4.6. Blocking access of the endpoints to the public DoH servers on the internet (such as PUBLIC RESOLVERS etc.).

10.3.2.4.7. Blocking access of the endpoints to public DoT servers on the internet (such as PUBLIC RESOLVERS etc.).

10.3.2.4.8. Blocking the ability of the user and/or an application to change the settings of the organizational DNS server (including DoT, DoH etc.) in the endpoints.

10.3.2.4.9. Adding relevant rules to the organizational monitoring mechanism (SIEM/SOC) for the purpose of detecting irregular access attempts.

10.3.2.4.10. Other.

10.3.2.5. The team is required to provide integration and support services regularly in accordance with the instructions set forth in this Tender.

10.3.2.6. The team is required to provide services in English as a minimum, and the Tender Holder will prefer team members who provide service in Hebrew.

10.3.2.7. The vendor shall be obligated to ensure that the team is informed regarding all malfunctions that are opened by the National Cyber Directorate and all managed organizations that receive the service within the framework of this Tender and, to the extent required, the team will be required to perform interior escalation.

10.3.2.8. The team is required to integrate the entire activities for the management of the service, its integration and the support vis-à-vis the National Cyber Directorate and the relevant managed organizations including functional issues relating to the service, for example: request to add intelligence feeds, requests to change the blocking algorithms, request for special reports, completion or coordination of training sessions, provision of functional trainings according to the questions/requests that the users present, providing professional service hours as may be required and in accordance with the Agreement, training, operation and support activities in organizations that connect to the service within the framework of this Tender (as part of the service envelope that is provided by the Bidder to the Directorate and to the organizations that will connect to the service), collection of feedbacks, positive and negative, from the tenants (managed organizations and single users), collection of requirements for future improvement and upgrade of the service and more. The team shall be the entity responsible for the active and regular integration of the service, including updates over time for the users, in coordination and under the control of the National Cyber Directorate.

10.3.2.9. The team is required to provide an initial response to any query of the Directorate and of the relevant managed organizations (other than the subject matter of the malfunction) regarding the infrastructure of the service as stated in this Tender.

10.3.2.10. The team will accompany the work of the users on behalf of the Directorate and on behalf of the managed organizations that connect to the service and shall assist to the employees of the National Cyber Directorate and the employees of the managed organizations in the service to maximize the quality of the deliverables that

are produced by the service while making optimal use of the capabilities of the service regularly and in connection with specific issues.

10.3.3. **Analysts**

10.3.3.1. **Mandatory requirements**

10.3.3.1.1. Analysts from the professional discipline subject matter of the Tender, i.e., DNS protocol.

10.3.3.1.2. Experience of 3 years as an analyst in the TI/TH world (in the field of DNS) with priority to former employees of cyber intelligence companies.

10.3.3.1.3. Priority to holders of international professional certifications in the worlds of TI/TH.

10.3.3.1.4. Verbal and written communication skills in English and/or Hebrew.

10.3.3.2. **Required work model**

10.3.3.2.1. An analyst on behalf of the Bidder is required to work 3 days a week in the offices of the National Cyber Directorate. Option to consider expansion of the position according to need, after six months. The expansion can be one additional workday per week in the Directorate offices, two additional days of work in the offices of the Directorate and/or additional options as may be required.

10.3.3.2.2. The analyst will have access to all the databases of the Bidder, subject to business limitations.

10.3.3.2.3. Primary objects of work

10.3.3.2.3.1. Sharing data and updates regarding new features of the service and giving proposals for their integration in the existing work processes in the Directorate.

10.3.3.2.3.2. Reviewing the different logs of the PDNS service itself and performance of research and detection tasks of anomalies, threats, deviations, deficiencies etc. and producing insights from these activities and making them accessible to the Directorate accordingly.

10.3.3.2.3.3. Development and advancement of new features for the service, including the submission of such requests in the name of the Directorate.

10.3.3.2.3.4. Externalizing existing intelligence information in the service provider for the Directorate, for example, cyber incidents around the world, sectorial cyber incidents, unique attack techniques that were found etc.

10.3.4. **Subcontractors**

10.3.4.1. The winning bidder shall be entitled to perform part of the activities by subcontractors.

10.3.4.2. The winning bidder is required to ensure, prior to the performance of the actions, that all subcontractors operating on its behalf have all valid approvals for the purpose of providing the requested Services, including required security clearances in the Tender.

10.3.4.3. In any event, the winning bidder shall be solely liable for the performance of the work, and any engagement of the entities on behalf of the Client in connection with the different works shall be made vis-à-vis the winning bidder.

10.3.4.4. The Tender Holder shall be entitled, at any stage, to demand the termination of the work of a subcontractor, for any reason, and without giving reasons. The winning bidder shall be required to provide the Services by itself or by another subcontractor.

10.3.5. **Security requirements from the team that will be employed by the vendor and the subcontractors that will be hired**

10.3.5.1. The Bidder shall deliver a list of relevant officers for the engagement, that will include the following information: name, family name, ID. No./Passport No., mobile phone, email.

10.3.5.2. The team members will undergo security checks for level 6 and checks confirming that they lack a criminal record.

10.3.5.3. It is necessary to obtain the approval of the Security Division in the National Cyber Directorate specifically for each team member.

10.3.5.4. The Security Division in the Directorate shall have sole discretion in defining specific employees who will be required to comply with unique security clearance requirements.

10.3.5.5. All relevant office holders will be required to arrive to a frontal security briefing. In this framework, they will be briefed regarding the data security guidelines and limitations in their conduct in the Directorate facilities.

10.3.5.6. All office holders that will be approved will be required to sign confidentiality statements and other declarations as a condition for the commencement of their employment.

10.3.5.7. In managed organizations wherein full-time support is required, and that will require physical presence in the Office facilities, integration and/or exposure to additional sensitive information, it is possible that the team members will be required to have a higher level of security clearance, as may be required and according to the instructions of the Security and Emergency

Division in the Directorate or in the managed organizations.

10.3.5.8. If additional office holders other than part of the team members that were defined by the Bidder and that were approved by the Security Division in the Directorate are required, the Bidder shall be required to deliver the list of these office holders for the purpose of conducting specific inspections by the Security and Emergency Division.

10.4. Replacement of office holders

10.4.1. The Tender Holder shall be entitled to demand the replacement of any office holder or a subcontractor on behalf of the winning bidder for any reason and without giving any reasons for its decision. In such circumstances as said, the winning bidder shall be required to make available another office holder whose identity will be approved by the Directorate and who complies with the requirements laid down in the Tender, and in the event that this is a subcontractor, to provide the services by itself or by another subcontractor who complies with the requirements laid down in the Tender.

10.4.2. Any replacement, whether initiated by the Tender Holder/Client and whether initiated by the vendor, shall be carried out with the approval of the Tender Holder and after delivery of a 30 workdays' advance notice or according to the advance notice period by law, whichever is earlier.

10.4.3. The new proposed office holder or the subcontractor is obligated to comply with the entire provisions set forth in the Tender.

10.4.4. The Tender Holder shall examine and approve the compliance of the new proposed office holder or the subcontractor with the requirements of the position.

10.4.5. The vendor shall not be entitled to use the services of the new office holder or subcontractor without obtaining the written approval of the Tender Holder.

10.4.6. The vendor shall provide full on-the-job training between the new proposed office holder or subcontractor and the outgoing one in a manner that will assure the uninterrupted performance of the requested services.

11. Functional-technological requirements

11.1. General requirements

11.1.1. The actions of the Bidder within the framework of this Tender including its products, the services and the software tools that will be operated within the framework of the Tender, to the extent that the Bidder wins the Tender, are performed and implemented in accordance with the provisions of the laws and statutes in the State of Israel, and the software, the products, the service or any other action of the vendor within the framework of the performance of the services for the Directorate under this Agreement shall not constitute any violation of the law including, but not limited to, in connection with intellectual property laws, computer laws and protection of privacy laws.

11.1.2. [M] The demand in this Tender is for a full SaaS service that is operated by the manufacturer of the system in the configuration operated by the manufacturer in its other regions around the world. It is clarified that the response should be in conformance to the existing configuration of the service on the submission date of the bids.

11.1.3. In this Tender the Tender Holder expects from the Bidder to use the strictest encryption standards in the protection of the service, the infrastructure in which the service is provided and the data, at rest and in motion.

Infrastructure requirements

11.2. [M] The vendor undertakes that the service shall be provided by the cloud service providers that won Central Tender 01-2020 for the provision of cloud services on a public platform for the government ministries and auxiliary units (hereinafter: the "Nimbus Tender") and undertakes that after setting up a data center in Israel by the cloud service provider with which it will engage – it will assure that all data relating to the services that are provided within the framework of this Tender will be transferred to the Israeli data center as stated hereunder.

11.3. [M] Deployment of the services in the Israeli region

11.3.1. The service that can be purchased under this Tender will operate from the Israeli region as an Israeli service, no later than December 31, 2024. The Tender Holder may exclude the vendor from this obligation, for a limited period of 6 additional months at the most, or 12 additional months, in the event that the service does not include content data.

11.3.2. The service shall be required to comply with all required standards and the SLA, in 6 additional months at the latest as of the date the service started being provided in the Israeli region.

11.3.3. The service will be operated in the Israeli territory according to the customary layout by the vendor for the service that is offered in other regions abroad where the service is implemented, and in any event will assure the survivability of the service and the continuation of its supply also in circumstances in which the domain is shut down.

11.4. [IM] manner of performance of the services during the setup stage

11.4.1. During the setup stage the Bidder shall be entitled to provide the services to the clients from an overseas region, in accordance with the rules and the conditions defined by the Tender Holder.

11.4.2. During the setup stage, the entire obligations set out in the Tender documents shall apply to the vendor, except for those that are conditional on the setting up of the services in the Israeli region.

11.4.3. The overseas region will be used as a temporary region in accordance with the provisions set forth hereunder. The Bidder is required to specify in each section accordingly:

11.4.3.1. The temporary region will be hosted in an overseas region when the payment for the services shall be made according to the overseas price list minus the percentage of discount set out in the Tender.

11.4.3.2. The temporary region shall provide work speed and delay as minimum as possible to the users from Israel

and will include a wide variety of cloud services and data security and cyber protection systems in the highest level customary in the Bidder and that facilitate uninterrupted, protected and reliable operation for the clients.

11.4.3.3. The temporary region will be defined as the default for the clients by virtue of this Tender, when the entire accounts, the users and the services that will be set up or operated in this region will be labeled as being part of the temporary region and will be subject to all the rules and the demands applicable with respect to the region.

11.4.3.4. After the establishment of the services in the Israeli region, the accounts and the bills that will be set by the Tender Holder will be migrated to the Israeli region based on the availability of the services in the Israeli region. The migration of the services and the accounts to the Israeli region will be performed without making a change in these accounts, except for automated reaffiliation to the Israeli region, if required, and with full and transparent transfer of the entire orders and commitments of the Tender Holder from the temporary region to the Israeli region, as if they were one region, including the migration of licenses, service orders per period (Reserves Instance, Committed use etc.), order balances, other commitments, credits Free (Credits) tiers and more that will be transferred in their condition "AS-IS" to the Israeli region without any reduction of the balance or the service or a demand for any additional consideration.

11.4.3.5. In the event that full migration cannot be performed as said, for any reason, the vendor shall provide an alternative solution for the service that will not be available in the Israeli region, will credit the Tender Holder or perform any other necessary action for the purpose of avoiding financial harm or harm to the

service level (for example: in the event it is impossible to transfer a service order for a period between regions, the vendor shall credit the Tender Holder with credits that will allow it to continue and receive the services within the framework of the commitment in the Israeli region for the remaining part of the period and for no additional cost in its behalf).

11.4.3.6. The Tender Holder shall be entitled to lay down, at its sole discretion, limitations and guidelines for use and consumption from the temporary region, while referring to considerations of security, privacy, and any other consideration that is relevant in its opinion.

11.4.3.7. The vendor shall assist, to the extent possible, to the Tender Holder and the clients for the purpose of meeting the requirements of the guidelines and the regulations applicable to them so that they can purchase services from the temporary region.

11.4.4. The vendor shall incur all costs for the transfer of data and any other customization work that is required for the purpose of operating the service fully from the Israeli region (whether these are computer resources, manpower or other).

11.4.5. The Bidder is required to specify the binding schedules and the major milestones for the purpose of setting up the services in the Israeli region until their full operation.

11.4.6. The Bidder is required to specify the risks in the process of setting up the services in the Israeli region and the measures that the Bidder applies for the purpose of handling these risks in order to mitigate the risk in the setup of the services in the Israeli region according to the schedule that the Bidder committed to.

11.5. Performance of the service in an overseas region

11.5.1. [IM] The Bidder is required to specify the capabilities of the temporary region with respect to the following matters:

11.5.1.1. The name of the hosting region that was selected and information regarding its features (number of domains, backup and survivability configuration, the services that are available in this region and any other additional information that might be help in the evaluation of the temporary region).

11.5.1.2. Model of operation of the temporary region, including the manner of linking the clients that are situated in Israel in order to minimize response times.

11.5.1.3. Describing the migration method of the systems from the temporary region to the Israeli region after completion of its setup, including the resources, the required costs (for example: data migration), downtimes etc.

11.5.1.4. Description of the migration method of the entire content, including policy settings, for example to the Israeli region.

11.5.1.5. Simultaneous operation capabilities of systems between the temporary region and the Israeli region during the migration period and the related costs.

11.5.1.6. Additional control and monitoring capabilities that will be made available to the Tender Holder.

11.5.1.7. Constraints and risks with relation to the governing law and the existing regulations in the temporary region that affect the purchase of the services and the upload of the protected data by the clients to the temporary region.

11.6. Configuration of the solution/system

11.6.1. [IM] The Bidder is required to specify the configuration of the proposed system while referring to the following issues:

11.6.1.1. The public cloud infrastructure on which the solution is based, out of the platforms offered by the cloud providers.

11.6.1.2. Whether the account on which the system operates is a unique account for the proposed system to the National Cyber Directorate within the framework of this Tender or whether it is shared by all clients/all tenants of the Bidder in Israel.

11.6.1.3. Manner of separation between the data of the different clients/tenants of the service, within the framework of the Tender and those outside this Tender.

11.6.1.4. Location and storage of the critical information on the Nimbus infrastructures and in the Israeli region.

11.7. Configuration of the work of the proposed service

11.7.1. [IM] The Bidder is required to specify the configuration of the operation of the proposed service while referring to the following issues:

11.7.1.1. Place of storage of protected data – in a "network" (such as VPC) of the Client/in the Bidder/in the manufacturer/other. In the event that the data is not stored by the Client, it is necessary to specify the location of its storage and the rules of its storage.

11.7.1.2. Place of processing of the content data in the "network" (such as VPC) of the Client/in the Bidder/in the manufacturer/other. In the event that the content data are not processed by the Client, it is necessary to specify the place of their storage.

11.7.1.3. If the storage of the materials and the processing are performed in the Client's premises, it is necessary to specify the access or the control capabilities of the

Bidder and the manufacturer over the data or the system, if any.

11.7.1.4. The Bidder is required to specify the configuration of the system connectivity to the Client's network with reference to the following issues:

11.7.1.4.1. Manner of connecting the Client's network in the cloud (such as VPC), it is necessary to specify whether the connection is, for example, in a configuration of Private Link, Peering, VPC Endpoint, the service is represented in the Client's network itself, through a VPN link or in any other manner, the manner of securing the connection and whether it is necessary to open external URLs for the purpose of making a connection to the service.

11.7.1.4.2. The interface that the management system of the service, it is necessary to specify whether the connection is, for example, in a configuration of Private Link, Peering, VPC Endpoint, the service is represented in the Client's network itself, through a VPN link or in any other manner, the manner of securing the connection and whether it is necessary to open external URLs for the purpose of making a connection to the service.

11.8. [IM] The data stored in the manufacturer/Bidder

11.8.1. The Bidder is required to specify the data that is stored in the manufacturer/Bidder during the performance of the services, such as processing data or subscription data. If part of these data is stored

outside the Israeli region, it is necessary to specify the place of their storage.

11.8.2. The Bidder is required to specify the data retention policy and the mechanisms that are implemented for the purpose of deleting the data when this is required.

11.8.3. To the extent that the manufacturer/Bidder retains data, it is necessary to specify the protective means of the data and the next tools and processes for the purpose of denying unauthorized access to the data.

11.8.4. Bidders are required to specify the process of granting access to these data and the groups of users who are entitled to view the data and the control processes for the purpose of detecting abuse of these permissions.

11.9. [IM] Configuration security and changes procedure

11.9.1. Bidders are required to specify according to what organized policy for configuration management and changes of all systems that participate in the performance of the services, according to the customary and the required standards, the manufacturer and the Bidder operate.

11.9.2. Bidders are required to specify the standard that is used for the purpose of performing these processes, to the extent that there is any, and provide a description in principle of the configuration control systems and the control process, confirmation, and documentation of changes.

11.9.3. Bidders are required to specify the controls for the prevention of unauthorized Downgrade of the encryption mechanisms, keys management mechanisms, protection systems or protection services, to the extent that there are any.

11.9.4. Bidders are required to specify the manner of protection and control in the development processes, such as secure software

development lifecycle (SDLC) and relevant standards, to the extent that the Bidder complies with these standards.

11.10. [IM] Limiting support access

11.10.1. The Bidder is required to specify the support process of the system, the supporting entities, whether these are entities on behalf of the vendor or the cloud provider and the process that is implemented in the vendor in the event there is a need for such access as said, including internal approval tracks, approval processes with the tenant, access security, the manner of its documentation (including session recordings, to the extent that there are any) etc.

11.10.2. The Bidder is required to specify whether it is possible to implement a mechanism in which any support access to the components that are used by the Client and that contain or that facilitate access to the processing data will be performed only after the implementation of a defined approval process wherein it will be necessary to obtain the approval of the representative on behalf of the Client for the support access.

11.10.3. Any access as said or an unauthorized access attempt will be recorded in an organized Log, including data regarding the accessing entity, data regarding the approving entity and any other relevant data. This Log will be accessible to the Client.

11.11. [IM] Risk management

11.11.1. The manufacturer/Bidder shall appoint an information security manager who will be responsible for securing the data in the proposed services, and will specify its job description, whether it is subordinated to the chief information security officer (CISO) or to the development manager or to any other entity, and a general description of the procedures according to which the said manager works.

11.11.2. The Bidder is required to specify the risk management processes in the organization.

11.11.3. The Bidder is required to specify the entities implementing these processes, the supervisory levels, the escalation license for handling the issues and the manner of handling of findings that were not handled.

11.11.4. The Bidder is required to specify the tools, means and the manner of their implementation for the purpose of allowing risk management in a dynamic manner and according to the changes in the outline of threats and in the services that are provided by the vendor.

11.12. [IM] Identification for the proposed service

11.12.1. Bidders are required to specify the support of the service in the SAML 2.0 protocol for the purpose of performing a Single Sign On with the Client's systems or central identification systems and support of Multi Factor Authentication. The Bidder is required to specify the support of the protocol and the support of additional identification protocols such as OAuth, OpenID.

11.12.2. The Bidder is required to specify the interface capabilities with IAM/idP tools (such as user management systems of the cloud providers with third-party systems such as OKTA, OneLogin, Azure AD) supported protocols (such as OTP, FIDO, U2F) etc.

11.12.3. The Bidder is required to specify the support of the password policy capabilities to the system users (including local users) that will include determination of variables such as: length, complexity, validity, password history etc.

11.12.4. The Bidder is required to specify the support of granting of access specifically in the role level RBAC – Role Bases Access Control, and in the attribute level ABAC – Attribute Based Access Control.

11.12.5. The Bidder is required to specify the support of the service in receipt of the data regarding the users from a central identification system in standard protocols.

11.13. [IM] Survivability and business continuity (SLA) of the proposed service

11.13.1. The SLA for the service that will be provided from the Israeli region will be no less than the SLA of any other region of the vendor and shall comply with the requirements laid down in this Tender (and in particular in section 12 of the Tender documents).

11.13.2. The Bidder is required to specify the control method over the quality of the service that is provided in the Israeli region and the escalation levels that are defined in the Bidder's procedures.

11.13.3. If backups are performed outside the cloud environment, it is necessary to specify the mechanism assuring the destruction of the memory base and obsolete components (such as their removal from the system, their replacement or in the event of a malfunction).

11.13.4. The Bidder is required to specify the options for backup or export of the content data to the base controlled by the Client regularly. The Bidder is required to specify the backup format and its compatibility to the standard systems in the market.

11.14. [IM] Protecting the vendor's infrastructures that are used for the purpose of providing the proposed service

11.14.1. The Bidder will specify the manner of monitoring of the systems in all aspects, 24 hours a day, 365 days a year, including reference to the following issues, as a minimum:

11.14.2. SIEM system;

11.14.3. SOAR system;

11.14.4. The entity that is responsible for monitoring and the entity performing the monitoring;

11.14.5. Reliable time source;

11.14.6. Integration capabilities in Zero Trust model;

11.14.7. Securing the endpoints;

11.14.8. Separation between different tenants;

11.14.9. The Bidder is required to specify the entire vendor's users or the subcontractors who can access protected data of the Clients or who have privileged access permissions such as: Administrators,

DevOps, Support, Operators etc. that will be monitored and identified in a high level. The Bidder is required to specify the work processes and the tools that are implemented by the vendor for the purpose of this matter.

11.14.10. The Bidder is required to specify the manner of protection of the processing data and the access of the tenants, including access control to the tenants, their encryption, the security tools protecting against unauthorized access or leak.

11.14.11. The Bidder is required to specify the manner of protection of the system management interfaces, separation between users, denying access of unauthorized entities, including the employees of the vendor or its subcontractors.

11.14.12. The Bidder is required to specify the manner of protection of the API interfaces of the system, internal and external.

11.15. [IM] Security tools used for the purpose of protecting the proposed service

11.15.1. The Bidder is required to specify the advanced and automated analysis tools, including AI integrated, for the purpose of detecting suspicious activities in the services provided to the users, attempts to expose or exposure of sensitive information etc.

11.15.2. The Bidder is required to specify the control, monitoring, and other cyber protection tools that the manufacturer uses, and that can be used by the Clients for the purpose of improving the protection of the information in their possession, such as DLP capabilities, handling malicious code etc.

11.16. [IM] Encryption and management of keys in the proposed service

11.16.1. The Bidder is required to specify the encryption capabilities of the data in the different service tiers including a response to the content data at rest and in motion, compensatory controls, if required, and the management of the encryption keys.

11.17. [IM] Collection of logs and monitoring

11.17.1. The Client may receive the entire processing and subscription data to its systems while supporting the transfer of the data to the SIEM systems of the Client, the Tender Holder or of a third party. The Bidder is required to specify the manner of transfer of the logs (online interface, periodic transfer of files, API etc.) on the SIEM systems that are supported and the scope of the support.

11.17.2. The Bidder is required to specify the possible log sources (such as: infrastructure, applicative infrastructure, application, information security etc.).

11.17.3. The Bidder is required specify the up-to-dateness of the data (the time from the occurrence of the event and until the transfer of the data), the scope of the data, the inquiry capabilities of the Client or its representative etc.

11.17.4. The Bidder is required to specify the period of time in which the processing data and the subscription data are stored by the manufacturer, the vendor's policy regarding the protection of these data and the manner of their protection.

11.18. [IM] Inquiry

11.18.1. The Bidder is required to specify the capabilities of the manufacturer/Bidder, its tools and work processes in the field of inquiry and response to cyber incidents in the systems of the manufacturer and/or the Bidder.

11.18.2. The Bidder is required to specify the tools and the services that the Clients have for the purpose of analyzing, inquiring, and responding to cyber incidents.

11.18.3. The Bidder is required to specify the process for operation of the Incident Response protocols, if there are any, in the event it is necessary to inquire security incidents, the involvement of cloud providers, response times, the resources available to the Client, interface configuration etc.

Service requirements

11.19. [M] The service will deny access to suspicious domains by denying the translation (Resolving) to their IP addresses.

11.20. [M] The service will permit the inspection of suspicious domains and decision-making regarding blocking, by the service, in a manual and automatic manner. The Bidder will specify the manner of use.

11.21. [M] The Bidder will allow the use of domains and IPv4 and IPv6 addresses according to the demands made by the Directorate, to which the DNS requests within the framework of the service will be directed.

11.21.1. [IM] The Bidder shall specify the use of the IPv6 addresses according to the demands made by the Directorate, to which the DNS requests shall be directed as part of the service.

11.22. [IM] The service will allow protection by identification as said. The Bidder is required to specify each section accordingly.

11.22.1. Malware and distribution/installation of malicious software (such as ransomware, viruses, spyware, fraud etc.).

11.22.2. Phishing attacks (for the purpose of identity theft, credentials theft, and other personal data and more):

11.22.2.1. Social Engineering Domain – use of malicious websites by making false promises for an upgrade, false positives etc.

11.22.2.2. Using incorrect spelling and/or replacement of letters in spelling (Character Substitution/Typo) squatting for the purpose of concealing access to websites with a low reputation level.

11.22.3. Use as a component in a command infrastructure (C2) for system-wide access to malicious websites and communication to C2C servers.

11.22.4. The use as component of Data Exfiltration.

11.22.5. Other.

11.23. [M] The service will classify assets of organizations, such as IP addresses and domains/sub-domains into Block Lists and Allow Lists also based on intelligence feeds.

11.23.1. [IM] The Bidder will specify the intelligence feeds that the service uses at present and their sources (the Bidder or a third party, and its identity).

11.23.2. [M] The service will integrate fully the use of intelligence feeds from a number of sources and in a number of formats, including data that will be provided by the National Cyber Directorate. It is emphasized that the full integration includes regular use of all intelligence feeds as basis for an update of Block Lists and Allow Lists.

11.23.3. [IM] The Bidder will specify the option to perform by the service the addition of data and/or intelligence feeds as basis for an update of the Block Lists and Allow Lists in different sections for different organizations:

11.23.3.1. [O] List of organizations that the Directorate will provide.
11.23.3.2. [O] All Israeli organizations.
11.23.3.3. [O] Sharing with all the service customers (not only those who receive the service within the framework of the engagement of the Bidder with the National Cyber Directorate).

11.23.4. [M] The service will support manual transfer of data such as domains for blocking, for example, by encrypted email, for integral integration in the service. The service will return confirmation regarding receipt of the data.

11.23.5. [IM] The Bidder will perform regular evaluation of the contribution of the intelligence feeds integrated in the service for the purpose of increasing the protection level of the organizations that use it and will present in a monthly breakdown the data to the National Cyber Directorate. The Bidder is required to specify the

manner of performing the evaluation and the manner of its presentation.

11.23.6. [M] The Bidder is required to receive updates and continue/remove regularly intelligence feeds (according to section 11.23.7) according to its evaluation regarding the contribution/removal from the performance of the service from the aspects of blocking, improving the False Positive levels, and more, and will update the National Cyber Directorate accordingly.

11.23.7. [O] Each input of intelligence feed will require the following:

11.23.7.1. [O] Transfer of the entire data that specifies the conformance of the intelligence feed and its expected contribution to the optimization of the service.

11.23.7.2. [O] Confirmation from the National Cyber Directorate.

11.24. [O] The service will enable monitoring only (Audit Only) of domains based on a Block List defined manually, by uploading a file (such as CSV), API or other. The Bidder will specify the implementation method.

11.25. [IM] The service will block domains based on a Block List that is configured manually. The Bidder will specify the implementation method.

11.26. [O] The service will block domains based on a Block List stemming from intelligence feeds (based on domain names, URLs and IP addresses, host names and more). The Bidder will specify the implementation method.

11.27. [IM] The service will allow a query by a user of the service regarding the domain that was blocked:

11.27.1. [IM] The query will be available at any time (24X7X365).

11.27.2. [IM] The query will be available by all available means for the purpose of receiving a service (telephone, email, portal and more, as stated in section 12.15.1.1).

11.27.3. [IM] The handling of the query will include a response to the user in the service and an update of the list accordingly.

11.28. [IM] The service will approve domains according to an Allow List that is defined manually. The Bidder will specify the implementation method.

11.29. [O] The service will approve domains based on an Allow List stemming from intelligence feeds (based on domain names, URLs and IP addresses, host names and more). The Bidder will specify the implementation method.

11.30. [O] The service will allow the blocking and approval domains also for international domains (IDN).

11.31. [IM] The service will also allow blocking and approval of domains based on the definitions in the Block List and Allow List for a limited period of time.

11.32. [O] The service will allow manual analysis of domain status including a response to its inclusion in the Block Lists, additional information regarding the level of the risk in using the domain, historic information regarding the domain and more.

11.33. [M] The service will handle False Positives – a domain that was blocked for an unjustified reason:

11.33.1. [IM] The Bidder is required to specify the manner of identification of the domains.

11.33.2. [IM] The Bidder is required to specify the manner of removal of the assets, such as the domains, from the Block Lists by the Bidder regularly and according to the demands made by the National Cyber Directorate or following the demand of the organization and with the approval of the National Cyber Directorate.

11.33.3. [IM] Reducing the level of False positives regularly. The Bidder is required to specify the method for performing this process.

11.33.4. [IM] The Bidder will specify the current level of False Positive of the service.

11.34. [IM] The Bidder will specify how the service handles the existing malicious methods and the existing threats (at least with the ones as stated in this section, however not limited to this section) and with new threats and methods:

11.34.1. [O] DNS request for orphan DNS servers, that are situated in a DNS/Domain/Sub-domain) that do not exist or that did not exist in the last 24 and/or 48 and/or 72 hours.

11.34.2. [IM] An algorithm for the creation of a domain (DGA).

11.34.3. [IM] New domain names and/or devices online (Domains, Host Names) that were created at least 24 hours and/or 48 hours and/or 72 hours and/or other retroactively and based on:

11.34.3.1. [IM] Regular intelligence update of the service on intelligence feeds.

11.34.3.2. [O] Custom compatibility, manual.

11.34.3.3. [O] Feed of automatic identifiers by the Directorate.

11.34.4. [IM] Data leak by DNS, such as DNS Tunneling (DNS Tunneling/Covert channel):

11.34.4.1. [O] Malware transmitted in encrypted traffic without the existence of a key in the protecting side.

11.34.4.2. [O] Data that leaks in encrypted traffic, without the existence of a key in the protecting side.

11.34.5. [IM] Protocol anomaly (for example, the size of each field and general size per query, order of data, types of Headers with respect to common requests, reputation of requests without a plausible explanation etc.).

11.34.6. [IM] Spike identification.

11.34.7. [IM] DNS Amplification attack.

11.34.8. [O] DNS Reflection attack.

11.34.9. [O] A DNS flood DDoS attack (NXDOMAIN Attack).

11.34.10. [IM] A cyber-attack against the service itself such as (however not limited to):

11.34.10.1. [IM] the Bidder is required to specify the penetration attacks to the service network.

11.34.10.2. [IM] The Bidder is required to specify DDoS attacks on the service based on volume rate per day, or based on a number of simultaneous requests per second (according to the changes in the threat environment), including a response to handling large-volume (volumetric) attacks, attacks against protocols and applications attacks, while using customary indicators such as throughput, number of requests per second (RPS), the period of time in which the infrastructure can handle an attack without sustaining a significant operational harm that will harm the service indicators that were set.

11.34.10.3. [O] Other.

11.34.11. [O] Response Rate Limiting (RRL).

11.34.12. [O] Limiting the number of requests at a given time from an IP address.

11.34.13. [O] Limiting the size of the DNS request/reply.

11.34.14. [O] Spoofing attack.

11.34.15. [O] DNS Poisoning.

11.34.16. [O] Interception in the regular translation and flow of data (Packet Interception).

11.34.17. [O] Authenticated Denial of Domain names.

11.34.18. [O] Free use of wildcards in domain names.

11.34.19. [O] DNS hijacking/DNS Redirection.

11.34.20. [O] DNS fast flux.

11.34.21. [O] ID guessing and query prediction.

11.34.22. [O] Betrayal by "trusted" server.

11.34.23. [O] Demand for detecting access to DNS record of the type that is not typical to the operations of a human user, for example TXT RECORD.

11.34.24. [O] Demand for tracking irregular content in DNS records such as TXT RECORD.

11.34.25. [O] Demand for blocking access to DNS records based on type, for example, it is impossible to inquire TXT RECORD.

11.34.26. [O] Demand for anonymous access when sending a DNS request abroad.

11.34.27. [IM] DNS Pseudo Random Domain Attacks.

11.34.28. [IM] BGP hijacking attack.

11.34.29. [O] Domain hijacking attack.

11.34.30. [IM] NXDOMAIN Attack.

11.34.31. [IM] Use of bots by attackers.

11.34.32. [IM] Malfunctions stemming from BGP redirection error, and common errors in application of configuration settings (misconfiguration).

11.35. [O] Block capabilities of domain names for the purpose of filtering content based on content categories (Content Filtering) such as betting, file sharing, illegal medications and drugs, and whether the service performs automatic cataloguing.

11.36. [I] the Bidder will specify the capabilities for tracing specific use in the level of the organization network:

11.36.1. [O] Tracing capabilities of the inter-organizational IP address of the computer that generated the original query.

11.36.2. [O] Tracing capability of the name of the inter-organizational user who generated the original query.

11.36.3. [O] Tracing capability of the inter-organizational MAC address that generated the original query.

11.36.4. [O] Whether there is a capability in accordance with section 11.36.1, whether there is an option to control the inter-organizational IP exposure according to demand or whether this is the service default.

11.36.5. [O] Whether there is capability, in accordance with section 11.36.2, whether there is also an option to control the exposure of the name of the organizational user according to demand, or whether this is the service default.

11.36.6. [O] Whether there is capability, according to section 11.36.3, whether there is an option to control the exposure of the organizational MAC address according to this demand or whether this is the service default.

11.36.7. [O] Whether there is capability, according to section 11.36.1, it is necessary to specify how the tracing is performed.

11.36.8. [O] If the capability in accordance with section 11.36.2 exists, it is necessary to specify how the tracing is performed.

11.36.9. [O] Protection capabilities against an attempt to create a DNS footprint (DNS Foot printing).

11.36.10. [O] Ability to know who is the active user who performed the original query and description of the manner of use.

11.36.11. [O] Option to implement a solution based on an intermediary (Proxy/Relay):

11.36.11.1. A demand for installation of software and/or hardware for the purpose of implementing this solution.
11.36.11.2. Additional and/or other demands for the purpose of implementing this solution.
11.36.11.3. Solution implementation method.
11.36.11.4. The Bidder is required to specify whether the solution can operate on customary virtual infrastructures such as VMware, Hyper-V, ESX and infrastructures of public cloud providers.

11.36.12. [O] The Bidder is required to specify whether the custom system/application has Resistance Tamper capabilities with implementation of an Evident-Tamper mechanism. If such capabilities exist, the Bidder is required to specify the implementation of these capabilities.

11.36.13. [O] The Bidder is required to specify capabilities for searching internal IP address following a request in the management screen and inherent search capabilities of the engine as said.

11.36.14. [O] The Bidder is required to specify the search capabilities of a username following a request in the management screen and the capabilities of the search engine to prevent such a search inherently.

11.36.15. [O] The Bidder is required to specify the search capabilities of a MAC address following a request in the management screen and the capability to deny such a search as said inherently.

11.36.16. [O] Other.

11.36.17. [O] The Bidder will specify whether the service allows the implementation of a permissions model that will allow to grant access to the organization regarding internal identifiers of the organization assets (such as the internal IP address, the MAC address, username) when the Directorate or another entity cannot be exposed to this information.

11.37. [O] The Bidder will specify the time of obsolescence of the records in the DNS server in which the requests are stored.

11.38. [O] The service will incorporate later on coping capabilities with developing threats and future attack techniques.

11.39. [O] The Bidder will specify the manner of implementation of the solution for a scenario in which there is communication disconnection between the State of Israel and the world, including a response to a scenario in which it is necessary to connect to the Israeli Internet eXchange that is maintained by the Israel Internet Association and in accordance with the instructions of the Association. This demand is relevant in circumstances in which, at the time of commencing the performance of the services, the cloud infrastructure that the vendor uses is not located in the Israeli region.

11.40. [I] The Bidder will specify the support of protocols, the version of the protocols and the manner of their use within the framework of the service:

11.40.1. [IM] DNS
11.40.2. [IM] DNSSEC
11.40.3. [IM] DNS over HTTPS (DoH)
11.40.4. [IM] DNS over Transport Layer Security (DoT)
11.40.5. [O] DNS-bases Authentication of Named Entities (DANE)
11.40.6. [O] DNSCrypt
11.40.7. [O] DNSCrypt v2
11.40.8. [O] DNSCurve
11.40.9. [O] ODoH
11.40.10. [O] DoQ (DNS over QUIC)
11.40.11. [O] DNS Certification Authority Authorization (CAA)
11.40.12. [O] STIX in its latest version for receipt/export of data
11.40.13. [O] TAXII in its latest version for receipt/export of data
11.40.14. [O] OpenIOC
11.40.15. [O] Other
11.40.16. [O] The Bidder will specify how the service enables work with DoT/DoH while performing authentication according to the following two alternatives (to be decided by the system administrator) – the user location and authentication data such as unique KEY.
11.40.17. [O] The Bidder will specify how the service enables work in Bring Your Own Key (BYOK) configuration such as work with DoH.

11.40.18. [IM] Support of update and/or integration in an integral manner of new protocols and new versions within the framework of the service that is provided fully and regularly.

11.41. [I] The Bidder will specify the support of standard and/or common DNS records and the manner of use within the framework of the service, such as:

11.41.1. [IM] A (Host address)
11.41.2. [IM] AAAA (IPv6 host address)
11.41.3. [O] ALIAS (Auto resolved alias)
11.41.4. [O] CNAME (Canonical name for an alias)
11.41.5. [IM] MX (Mail eXchange)
11.41.6. [IM] NS (Name Server)
11.41.7. [O] PTR (Pointer)
11.41.8. [IM] SOA (Start of Authority)
11.41.9. [O] Other

11.42. [I] The possible responses to translation requests will be the following as a minimum:

11.42.1. [M] Enforcement of the redirection to a block page with a message to the user of the service.
11.42.1.1. [IM] The Bidder will specify the options for the user messages in the service.
11.42.1.2. [O] The service will permit customization of the block page according to the demands made by the National Cyber Directorate (for example – the Directorate logo, instructions for certain actions, reason for the blocking, request for support and more).
11.42.1.3. [O] The service will allow support of messages in different languages. The Bidder is required to specify the supported languages.
11.42.1.4. [O] The Bidder will specify the structure of the message for a request that was blocked, for the purpose of transferring by API with respect to the following (as a minimum):
11.42.1.4.1. [O] Data in the network/protocol level (date, time, IP address of the requesting source, port of the requesting source, the

device/website of the requesting source, name problem query, type of query, query class)

11.42.1.4.2. [O] Data regarding a malicious domain (source of the intelligence feed, if known, type of malware, name of malware, rating/level of influence, if known)

11.42.1.4.3. [O] Additional relevant data that might enrich the data and strengthen the block.

11.42.2. [M] No redirection (NXDOMAIN message)

11.42.3. [O] Enforcing the redirection to the sinkhole server

11.42.4. [O] Other

11.43. [O] The service will allow the collection of data (such as access to websites) in a departmentalized manner between different managed organizations (multi-tenants). The Bidder is required to specify the manner of implementation.

11.44. [O] The service will allow support in balancing a global server load (GSLB/GLBS/GeoDNS) including a response of the secondary server to the main server and vice versa and data regarding the service data (required time for the transition and more).

11.45. [O] The service will allow display of incidents/suspected incidents according to the MITRE ATT&CK work model in its latest version.

11.46. [O] The service will allow display of the protection mechanisms that were activated in response to incidents/suspected incidents according to the MITRE D3FEND Matrix in its latest version.

11.47. [O] The service will allow a display of the protection mechanisms that were activated in response to incidents/suspected incidents according to the incidents/suspected incidents according to the NIST Cybersecurity framework in its latest version.

11.48. [M] The service will allow the definition of a policy in the level of the State, sector, activity and organization including downscaling to the level of the single

organization and determination whether this is a mandatory policy category for each level under the defining level or whether it is optional (in such manner that the level of the activity sector and/or organization level can define a custom policy that is different than the one that was defined in the level of the state and/or the sector of the activity, respectively). The Bidder will specify the implementation options, including a response to the affiliation of a domain/IP address to the Block List or Allow List according to the policy of each organization.

11.49. [O] The Bidder will specify the service capabilities for support of remote work (Roaming Clients):

11.49.1. [O] The possible measures for the purpose of supporting remote work including support of computers, mobile phones, tablets and supported operating systems (Windows/Linux/IOS/Android and more).

11.49.2. [O] The use of custom tenant configuration (for example, branding block messages, tenant/service branded as a tenant/service of the National Cyber Directorate).

11.49.3. [O] The Bidder will specify whether the application service for support of remote work (Roaming Clients) has Resistance Tamper capabilities while implementing a mechanism for exposing such tampering (Evident-Tamper). If such a mechanism exists, the Bidder is required to specify its capabilities.

11.49.4. [O] The Bidder will specify the support options in circumstances in which the internet service provider does not grant access to external DNS servers (for example, HotSpot).

11.49.5. [O] The Bidder will specify the option for defining safe networks such as circumstances in which the user of the service is in the office network (Trusted Network).

11.50. [IM] The Bidder will specify the retention and export capabilities of all DNS requests including all their data and the replies provided for them.

11.50.1. [IM] The Bidder will specify the data export features including a response to all the export interfaces, exportable data and more.

11.50.2. [O] The Bidder will specify the option to block usage without receiving the data regarding the usage of the user or its encryption.

11.50.3. [O] The Bidder will specify the option for a configuration that allows to the holder of the device to shut down the service independently (for reasons relating to privacy).

11.51. [IM] The Bidder will specify whether the consumption of the service by the tenants is not conditional on the performance of an installation of a software component (including a virtual appliance) or hardware in the tenant's premises.

11.52. [I] Management capabilities of the service and interfaces

11.52.1. [I] The service ought to provide a response to different types of users in the service/organizational levels as follows:

11.52.1.1. [M] **Managed organizations' manager of the service (the National Cyber Directorate)** – will be able to engage in management of all managed organizations (Multi Tenants) including the National Cyber Directorate, for example, add and remove managed organizations, managing all the service capabilities, including definition of policy and records, viewing and analysis capabilities of the entire data in a centralized manner etc. by the service management interface.

11.52.1.2. [M] **The manager of a group of managed organizations that will be added to the service** – will be able to manage the data of organizations included in the group, including an updated policy based on basic policy on behalf of the managed organizations' manager of the service (the National Cyber Directorate), add and remove managed organizations, add and remove organizational users according to the

authorization level that will be assigned to the said user of the service, and will be able to perform actions in the service independently (self service). The group of organizations will be structured by the group manager by the service interface.

11.52.1.3. [M] **The manager of a single managed organization that will be added to the service** – will be able to manage the data of the said organization, including updated policy based on a basic policy on behalf of the managed organizations' manager of the service, add and remove organizational users according to the permission level that will be granted to the said user of the service, and will be able to perform actions in the system in an independent manner (Self service).

11.52.1.4. [M] **A user in a managed organization** - will be able to manage the data of the organization to which it belongs according to the permission level that will be defined for it in the service, and will be able to perform actions in the system independently (Self service).

11.52.1.5. [M] The service will include users of types that enable the performance of the required actions according to the definition of the type of the user in this Tender for the entire engagement:

11.52.1.6. At least 300 users of the type user on behalf of a managed organization.

11.52.1.7. At least 300 users of the type manager of a single managed organization.

11.52.1.8. At least 10 users of the type manager of a group of organizations.

11.52.1.9. At least 5 users of the type managed organizations' manager.

11.52.2. [M] The service will make accessible to the service user proper **interfaces** (Portal and API) that will facilitate the performance of the entire actions as stated in this Tender, without limitation on the number of API queries for each user in the service and for all users in the service according to the requirements of the Directorate and the organizations that will use the service.

11.52.3. [O] The service will include a separation between APIs that serve the end customers and APIs that serve the Directorate and managed organizations that the Directorate will define. The Bidder is required to specify the implementation method.

The Bidder will specify in the table the service capabilities in a breakdown to the type of user and the manner of implementation of these capabilities by the proper management interface:

Type of user/section no.	Classification of requirement	**Description of the service capability and manner of its operation** (in the level of the National Cyber Directorate/group of managed organizations and in the level of the managed organizations)	Managed organizations' manager of the service	Manager of a group of managed organizations	Manager of a managed organization	User in a managed organization
11.52.3.1	[IM]	Managing the permissions hierarchy – manner of exposure to the entire service capabilities according to the types of users and the option to update the permissions				
11.52.3.2	[IM]	Addition and removal of managed organizations				
11.52.3.3	[IM]	Addition and removal of users of the service				
11.52.3.4	[IM]	Addition and removal of endpoints in the service				
11.52.3.5	[IM]	Management viewing and editing capabilities				
11.52.3.6	[IM]	Management and analysis capabilities of D&I (Detection and Identification) data of the National Cyber Directorate/group of managed organizations and of the managed organizations				
11.52.3.7	[IM]	Retrieval of the D&I data of the managed organizations by API				
11.52.3.8	[IM]	Defining a Block List and an Allow List				

11.52.3.9	[IM]	Update of Block List and Allow List				
11.52.3.10	[O]	Defining internet usage policy (for example, RPZ – response policy zones)				
11.52.3.11	[O]	Addition of RPZ according to demand by API				
11.52.3.12	[IM]	Support of the operation interface in English and/or Hebrew				
11.52.3.13	[IM]	Support of the operation interface in English and/or Hebrew				
11.52.3.14		Registration fees of user in electronic method (Self Service) including validation test				
11.52.3.15	[O]	Integration of human testing				
11.52.3.16	[O]	Inspection of affiliation of the assets to the data registered				

11.52.4. [M] the service will make accessible to all organizational levels described in this document (general management, management of a group of organizations, a single user organization, other) on demand and periodically (as defined by the National Cyber Directorate) all **logs** that the service generates:

11.52.4.1. [IM] The Bidder will specify the data that are saved in the logs of the service and that can be exported from it.

The logs will include all DNS queries and the answers that will be provided, whether or not the query was approved, blocked, altered, and whether a message that domain does not exist or another message was received.

11.52.4.2. [IM] The Bidder will specify the means for the purpose of exporting logs from the service:

11.52.4.2.1. [M] API

11.52.4.2.2. [O] The service interface (portal and/or the management interfaces)

11.52.4.2.3. [O] Other (the Bidder is required to specify)

11.52.5. [M] The service will allow the user to receive structured data, search in it forms and patterns and, in addition, an option to export the data (Translation requests, blocks, Block List and Allow List, intelligence feeds, activity history and more) by a full and unlimited API to the system that the Directorate uses. The data will be used by all units in the Directorate for the purpose of performing its tasks. (While using the capabilities of a Passive DNS domain name as part of the DNS work method). The Bidder will specify the possible period of time for a historic search.

11.52.6. [IM] The service will create **notifications** regarding changes in the data (for example a change in the Block List, a change in the policy of a managed organization, a change in the composition of intelligence feeds and more) according to the decision of the service user, shortly after the update time of the data, and will report them to the user by push notifications.

11.52.6.1. [IM] The service will notify the managed organizations' manager about the detection of incidents that might be of interest:

11.52.6.1.1. [IM] The Bidder will analyze the data of the service over time for the purpose of defining criteria for the identification of incidents that might be of interest to the National Cyber Directorate (while

working in cooperation with and making the criteria in conformance to the criteria of the National Cyber Directorate).

11.52.6.1.2. [IM] The service will send notifications regarding incidents that might be of interest to the National Cyber Directorate in 30 minutes at the most from the time of detecting the incident.

11.52.6.1.3. [IM] The notification will also include the incident metadata.

11.52.6.1.4. [O] The service will perform a similar process to the process described in this section for other organizations that are connected to the service within the framework of this Tender.

11.52.6.2. [IM] The service will notify the different types of the users of the service according to the type of the notification and the notification itself:

11.52.6.2.1. [IM] The Bidder will specify the existing notifications in the organizational level/types of the different service users:

11.52.6.2.1.1. [IM] Blocking the domain and the reason for its blocking

11.52.6.2.1.2. [O] Crossing the threshold for a number of queries for a domain that was blocked in different organizational levels

11.52.6.2.1.3. [O] In the event that the website is active only in the last 48 hours and the domain was registered only in the last 72 hours

11.52.6.2.1.4. [O] Irregular queries, for example queries that were not made in the last 30 days

11.52.6.2.1.5. [O] A number of unreasonable DNS queries at a specific time (for example, more than 200 per hour)

11.52.6.2.1.6. [O] Other

11.52.6.3. [I] The service will allow the user of the service to select the following:
- 11.52.6.3.1. [O] The factors for the change that will generate notifications
- 11.52.6.3.2. [O] The threshold for the change to generate notifications for each relevant change factor
- 11.52.6.3.3. [O] The target of the notification (for example, according to a specific type of user, a specific user, a group of users)
- 11.52.6.3.4. [O] Medium for transmission of the notification (for example, portal and/or email and/or WhatsApp and/or API, other).
- 11.52.6.3.5. [O] Other

11.52.6.4. [I] The notification will be transmitted by the following reporting media:
- 11.52.6.4.1. [IM] The service portal
- 11.52.6.4.2. [IM] Email
- 11.52.6.4.3. [O] API interface
- 11.52.6.4.4. [O] WhatsApp interface
- 11.52.6.4.5. [O] Support of WEBHOOK (query protocol, method for transmission of messages by WEB)
- 11.52.6.4.6. [O] SIEM systems or other systems
- 11.52.6.4.7. [O] Mobile application – custom or based on a third-party application
- 11.52.6.4.8. [O] The Bidder will specify other options

11.52.6.5. [I] The following general data will be displayed in addition to the content of the notification:
- 11.52.6.5.1. [IM] The notification time
- 11.52.6.5.2. [O] Other

11.52.6.6. [I] Unique notifications:
- 11.52.6.6.1. [IM] The Bidder will specify the capabilities for sending a notification to

a user in connection with an unusual translation request

11.52.6.6.2. [O] Notifications prior to the extension/termination of the service according to the definition of the managed organizations' manager

11.52.6.6.3. [O] The service will notify that a specific organization is inactive for a specific period of time

11.52.6.6.4. [O] The Bidder will provide additional and structured unique notifications

11.52.7. [I] The service will allow the user to export manually and automatically (by way of retrieval or push) a **report** based on the data that is relevant to the organization or to the group of organizations according to the decision made by the user and the user's permissions. The service will give the option to include different items of data in the report.

11.52.7.1. [IM] The Bidder will present all the possible reports in the service and their data.

11.52.7.2. [I] The user will be able to create a report according to the following information:

11.52.7.2.1. [IM] Translation requests and blocking based on the organization's name

11.52.7.2.2. [IM] A report in English

11.52.7.2.3. [O] A report in a format customized to MITRE

11.52.7.2.4. [O] A report customized to the user's requirements

11.52.7.2.5. [O] A regular information report to an organization and/or a sector and/or a state (for example, containing statistical data, interviews and blocking etc.)

11.52.7.2.6. [O] An automated scheduled report

11.52.7.2.7. [O] TOP 10 websites that were blocked

11.52.7.2.8. [O] TOP 10 ranked websites

11.52.7.2.9. [O] TOP 10 IP addresses that were part of internet inquiry (based on the number of inquiries)

11.52.7.2.10. [O] TOP 10 IP addresses that were blocked (based on the number of domains that were blocked)
11.52.7.2.11. [O] A daily report of performance indicators
11.52.7.2.12. [O] A daily report of blocking percentage
11.52.7.2.13. [O] A daily report of the number of queries and relevant attributes
11.52.7.2.14. [O] Structure updates and information regarding the said reports over time, as may be required
11.52.7.2.15. [O] Reports in Hebrew
11.52.7.2.16. [O] Reports in English

11.52.7.3. [IM] The service will allow the user to produce a report as stated in this section, in at least one of the following formats, and the Bidder will specify the possible formats:
11.52.7.3.1. Word
11.52.7.3.2. PDF
11.52.7.3.3. CSV
11.52.7.3.4. HTML
11.52.7.3.5. JSON
11.52.7.3.6. Other

11.52.7.4. [IM] The service will allow the user to save the report as stated in this section as a file in the local computer.

11.52.8. [M] The service will allow **import and export** as stated in this section as a minimum.
11.52.8.1. [IM] Data for import and export:
11.52.8.1.1. [IM] Block Lists
11.52.8.1.2. [O] Allow Lists
11.52.8.1.3. [O] List of managed organizations
11.52.8.1.4. [O] List of users (in the organization, in a group of organizations, all users)
11.52.8.1.5. [O] Reports as stated in this section
11.52.8.1.6. [O] Other

11.52.8.2. [IM] The service will allow manual and electronic import and export (by way of retrieval and push) of data (for example, Block List):
11.52.8.2.1. [IM] By an API portal
11.52.8.2.2. [O] the service portal
11.52.8.2.3. [O] Other
11.52.8.3. [O] The import and export capabilities of the service can work in one-directional configuration and use one-directional protocols.
11.52.8.4. [IM] The Bidder is required to attach to its bid an appendix containing answers to this section that includes full documentation of the API interface.

11.52.9. [IM] The service will provide **operational reports** by Dashboard screens and reports, and the Bidder will specify the structure and the content of the screens and the reports by the different management interfaces while responding to the different organizational levels, as stated in this Tender, and according to different filtering features (for example in different time sections (time, day, week, month)):
11.52.9.1. [IM] Data regarding joining to the service in different organizational levels, sectors and more
11.52.9.2. [IM] Data regarding use and browsing for a user of the service, including volumes of use of the network, according to the demand of the National Cyber Directorate
11.52.9.3. [IM] The Bidder will specify the option of reflection of screens (dashboards) for the purpose of displaying the usage data as stated in this section for the users of the service in different organizational levels by the service management interfaces (for example, sector, single organization, single user)
11.52.9.4. [IM] Status of use of the different organizational levels (logging in to the service portal, transfer of Translation requests and more)
11.52.9.5. [IM] Regularity of the blocking and redirection mechanisms in all organizations.
11.52.9.6. [O] Status of use of the different service resources:

11.52.9.6.1. [O] Bandwidth consumption per hour
11.52.9.6.2. [O] Trends over time (monthly, annual)
11.52.9.7. [IM] Block List and Allow List
11.52.9.8. [O] Update regarding the removal of a domain from the Block List and the reason for this.
11.52.9.9. [O] Number of queries from a computer per hour.
11.52.9.10. [O] Statistical data of types of queries in a breakdown to time (daily, monthly, annual) and organizational section.
11.52.9.11. [O] Configuration errors.
11.52.9.12. [O] Indication regarding the presence of malware.
11.52.9.13. [O] Percentage of queries that are blocked out of all queries from the same source (device, IP address, organization and more) in a breakdown to time (week, month, year).
11.52.9.14. [O] Other

11.52.10. [IM] The Bidder is required to allowed **integration** of the service with systems and tools, to the extent that these have a standard and customary interface.
11.52.10.1. [IM] To the extent that there are software products, intelligence feeds and third-party services in respect of which there is integration and/or a link to the API interface of the Bidder for the purpose of expanding the service, it is necessary to specify them.
11.52.10.1.1. [IM] Interface with different SIEM systems (for example Google Cyber/Splunk/QRadar/Shield/ASO) in the different levels of management/organization.
11.52.10.1.1.1. [IM] The Bidder will specify whether there is structured integration or another interface for the SIEM systems and to which SIEM systems.
11.52.10.1.1.2. [IM] The Bidder will specify the options for use and all data transferred by the interfaces referred to in the previous section, including information regarding the interfaces, dashboards and more.

11.52.10.1.1.3. [IM] If there is no structured integration or any other interface, the Bidder is required to specify whether this is planned for implementation, for what system and when.

11.52.10.1.1.4. [O] Implementation of Sinkhole or performance of integration for such capability.

11.53. [IM] The Bidder will specify whether the service is structured in such manner that it includes the option to customize and add capabilities and interfaces in each of the stages of the process according to the requirements of the National Cyber Directorate.

11.53.1. [IM] The Bidder will specify how the process for the addition of capabilities and interfaces is structured. In this regard, the Bidder will specify the following –

11.53.1.1. [IM] Whether the addition of the capabilities should and/or can be performed by the Bidder only, by the tenant only or a combination of both.

11.53.1.1.1. [IM] If implemented by the Bidder only or jointly with the tenant, whether it is necessary to purchase hours of professional services (PS) that will be provided by technology experts or development hours or as a full customization project on behalf of the Bidder. Example of additions – development of unique capabilities, customizations for the user's requirements, writing customized scripts (code segments/scripts), API customizations as may be required and more.

11.53.1.2. [O] Intelligence products/feeds (including off-the-shelf, proprietary products or open-source products) that the Bidder can purchase and integrate in the service. The Bidder will specify the products and the option of their integration in the service and/or in its management interfaces.

11.53.1.3. [O] Options to customize the management interfaces to the requirements of the National Cyber Directorate.

11.53.1.4. [O] Option to integrate in the service and in the management interfaces of the service products that will be purchased or that are used by the Directorate. The Bidder will specify how or with what measures it is possible to integrate them in the service and/or in its management interfaces.

11.53.1.5. [O] Option for the service to interface with the national cyber services portal of the National Cyber Directorate by API and/or by other customary (standard) interface measures that the Bidder will specify.

11.53.1.5.1. [O] Each interface between the service and its management interfaces to the Directorate portal will allow full and two-directional transfer of data of the entire service data and its management interfaces as stated in this Tender.

11.53.1.5.2. [O] the service data (telemetry of requests and the translation answers accordingly) will be transferred in whole or in part, in coordination with the National Cyber Directorate.

11.53.1.5.3. [O] Integration with the Directorate portal in different fields such as SSO, permissions management and more.

11.53.1.6. [O] Options for the development of a custom portal that will be developed later on, as may be required, based on the information provided within the framework of the services. In this section the Bidder will specify, among other things, also the options for developing the custom portal in Hebrew and/or in English, the option to add a logo, option to add an identification mechanism and manual confirmation and more.

11.54. [I] The service will allow the user to make personal customization to its work environment in the system (personalization) and in this regard:

11.54.1. [O] The creation and management of notifications, as stated above.

11.54.2. [O] The creation and management of reports, as stated above.

11.54.3. [O] The Bidder is required to specify other personalized features that are supported in the system.

11.55. [IM] The service shall comply with customary standards in the field of data communication, cyber protection, and data security, such as IETF RFCs. The Bidder will specify and demonstrate the standards that the service complies with.

11.56. [IM] The Bidder will be able to provide a direct demonstration (Live Demo) by the service, in its official version (Stable Release/GA) including presentation of the results in the user interface (UI/Portal) in a report and in API the scenarios described in the Excel file attached (under classification [M], [IM] and [O]). Explanations and additional demands will be provided during the technological stages of the Tender (demo and pilot) as may be required, according to examples that will be given in advance by the National Cyber Directorate and according to its instructions, in a uniform manner to all Bidders.

12. Support and Operation Requirements and Response Times

[I] This section including sub-sections thereof specifies the minimum requirements for support and operation of the proposed service. the Bidder is required to specify with respect to each of the sections how the proposed service supports the Tender requirements.

12.1. Availability of service

12.1.1. The service availability (the protection system) will be 24 hours a day, 7 days a week, except for short, scheduled downtimes for maintenance and upgrade purposes in respect of which a notice of no less than one week in advance shall be delivered. The total availability on annual average will be no less than 99.999% including during a cyber-attack on the vendor's infrastructure and including during the time of an operational malfunction in the vendor's systems and the systems on which the vendor relies. The Bidder shall specify the total availability of the service on annual average.

12.1.2. The availability of the management interfaces of the service (management services for the different organizational levels, update of the Block Lists etc.) will be 24 hours a day, 7 days a week, except for short, scheduled downtimes for maintenance and upgrade purposes in respect of which a prior notice of no less than one week will be delivered. The total availability on an annual average will be no less than 95%. The Bidder will specify the total availability of the service on an annual average.

12.1.3. The service may operate independently and without interrupting functionality in the event the State of Israel is disconnected from the worldwide web. Whether the incident stems from a technical malfunction, a cyber incident or for another reason.

12.1.4. Technical support may be provided by the dedicated integration and support team on behalf of the Bidder (as stated in this chapter)

with at least one year of experience, 24 hours a day, 7 days a week, 365 days a year.

12.1.5. [A] Business continuity indicators for the service:

12.1.5.1. 0 = RPO Recovery point objective (no loss of data. Whether this is an incident stemming from a technical malfunction, a cyber incident, or another reason).

12.1.5.2. 4hr = RTO - Recovery Time Objective.

12.2. Repairing malfunctions in the service

12.2.1. [I] Types of malfunctions

12.2.1.1. "Disabling" malfunction

A malfunction that disables the entire service or material parts of the service and/or that does not allow the use of the service or material parts of the service and/or that seriously disrupts the service that is consumed.

12.2.1.2. "Major" malfunction

A malfunction other than a disabling malfunction, as hereinafter defined, and that causes a disruption in the use of specific parts of the service and/or that does not allow users to continue and use the service fully and/or a malfunction that causes a response time that is unreasonable.

12.2.1.3. "Regular" malfunction

A malfunction other than a disabling or a major malfunction, as hereinabove defined, for example minor disruptions in the normal use and operation of the service. Such a malfunction is caused as a result of lack of operation or lack of availability of a function or a component in the service that is not required on a daily basis or that is not used regularly.

12.2.1.4. "System-wide" malfunction

A malfunction that harms the infrastructures of the service or that affects at least two tenants simultaneously.

12.2.1.5. "Local" malfunction
A malfunction that does not harm the service infrastructures or the Bidder's infrastructures and that affects only one tenant.

12.2.2. The opinion of the Directorate shall be decisive in any dispute regarding the type of the malfunction.

12.3. [IM] Required response and service times (SLA)

The Bidder undertakes to meet the response and service times for the types of the malfunctions as stated in this section. The Bidder will specify its compliance with this section, and to the extent that the Bidder offers SLA within the framework of the service, the Bidder is required to attach the proposed SLA. In any event, the SLA shall not fall below the standard SLA terms that are offered to the customers of the Bidder's service.

System-wide malfunction in the service itself (the entire service or in the majority of the connected organizations):

Type of query/malfunction	Response time for commencement of handling of the query/malfunction	Maximum period of time for solving the malfunction	Comments	Compensation amount
Disabling malfunction	Immediately after receiving the notice	Up to one calendric hour from the time of receiving the notice	Handling the malfunction continuously, irrespective of time intervals (also not during the regular hours of work) and until the malfunction is fully repaired to the satisfaction of the National Cyber Directorate (including at night, on statutory, Saturdays and holidays as of the start of the Sabbath/holiday and until their end)	ILS 5,000 per malfunction If the malfunction was not handled in 3 hours, the amount of compensation will increase to ILS 1,000 per hour for a malfunction that was not handled.

Type of query/malfunction	Response time for commencement of handling of the query/malfunction	Maximum period of time for solving the malfunction	Comments	Compensation amount
Major malfunction	30 minutes from the time of receiving notice	2 hours from the time of receiving notice	Handling the malfunction continuously, irrespective of time intervals (also not during the regular hours of work) and until the malfunction is fully repaired to the satisfaction of the National Cyber Directorate (including at night, on statutory, Saturdays and holidays as of the start of the Sabbath/holiday and until their end)	ILS 2,500 per malfunction If the malfunction was not handled in 4 hours the compensation amount will increase to ILS 500 per hour for a malfunction that was not handled.
Regular malfunction	In 2 hours from the time of receiving notice	4 hours from the time of receiving notice	Handling the malfunction continuously (also not during the regular hours of work) and until the malfunction is fully repaired to the satisfaction of the National Cyber Directorate (including at night, on statutory, Saturdays and holidays as of the start of the Sabbath/holiday and until their end)	ILS 1,250 per malfunction If the malfunction was not handled in 8 hours the compensation amount will increase to ILS 250 per hour for a malfunction that was not handled.

<u>Local</u> malfunction in the service itself (in a specific organization or a series of organizations):

Type of query/malfunction	Response time for commencement of handling of the query/malfunction	Maximum period of time for solving the malfunction	Comments	Compensation amount
Disabling malfunction	Immediately after receiving notice	1 hour from the time of receiving notice	Handling the malfunction continuously, irrespective of time intervals (also not during the regular hours of work) and until the malfunction is fully repaired to the satisfaction of the National Cyber Directorate (including at night, on statutory, Saturdays and holidays as of the start of the Sabbath/holiday and until their end)	ILS 2,500 per malfunction If the malfunction was not handled in 3 hours, the compensation amount will increase to ILS 500 per hour for a malfunction that was not handled.
Major malfunction	In two hours from the time of receiving the notice	4 hours from the time of receiving the notice	Handling the malfunction continuously, irrespective of time intervals (also not during the regular hours of work) and until the malfunction is fully repaired to the satisfaction of the National Cyber Directorate (including at night, on statutory, Saturdays and holidays as of the start of the Sabbath/holiday and until their end)	ILS 1,250 per malfunction If the malfunction was not handled in 6 hours, the compensation amount will increase to ILS 250 per hour for a malfunction that was not handled.
Regular malfunction	In 4 hours from the time of receiving the notice	6 hours from the time of receiving the notice	Handling the malfunction continuously, irrespective of time intervals (also not during the regular hours of work) and until the malfunction is fully repaired to the satisfaction of the National Cyber Directorate (including at night, on statutory, Saturdays and holidays as	ILS 800 per malfunction If the malfunction was not handled in 8 hours, the compensation amount will increase to ILS 150 per hour for a malfunction that was not handled.

			of the start of the Sabbath/holiday and until their end)	

12.3.1. The Bidder shall repair malfunctions in the service immediately after detecting the malfunction independently or after receiving a notice from the National Cyber Directorate, whichever is earlier, and will act continuously until the malfunction is repaired fully according to the malfunction categories according to the principles set out in this section.

12.3.2. The Bidder will update the National Cyber Directorate immediately after detecting a malfunction in the service and will update the Directorate regularly while handling the malfunction.

12.3.3. The Bidder is required to specify the manner of communication of the information regarding the malfunction and the manner of handling the malfunction to the National Cyber Directorate while providing the information regularly when handling a disabling malfunction and a major malfunction.

12.3.4. The Bidder is required to specify the query and reporting methods about malfunctions in the service.

12.4. Response times to the service

12.4.1. [IM] The proposed service infrastructure and the integration and support team will meet the following response times, as a minimum:

Action	Maximum response time	Malfunction classification
Initial login to the management screen	15 seconds	Regular malfunction
Reloading a screen	15 seconds	Regular malfunction
Update of list (addition/removal of a domain)	45 minutes from the time of the request	Major malfunction

Action	Maximum response time	Malfunction classification
Update of list (addition/removal of a domain) based on information and/or intelligence feed that was provided by the National Cyber Directorate	45 minutes from the time of the request	Major malfunction
Query of a user of the service regarding a domain that was blocked/a domain that was not blocked	45 minutes from the time of the query	Major malfunction
Removal of a domain that was identified as a false positive from the Block List	45 minutes from the time of detection	Major malfunction
Presentation of new information that was created in the service by the interface (portal and API)	15 minutes from the time the information is created	Regular malfunction
Production of a standard report or presentation of dashboard	45 seconds	Regular malfunction
Production of a complex report	5 minutes. The user will receive a notification stating that a long action is performed, and indication regarding the status of progress.	Regular malfunction
Response time for API interface	Single query – 20 seconds Collection of hundreds of queries – 2 hours	Major malfunction
General response of the integration and support team	4 hours on workdays	Major malfunction
Answers to specific and operational questions by the integration and support team – National Cyber Directorate	2 hours (24*7)	Major malfunction
Answers to specific and operational questions of the integration and support team – managed organizations	4 hours (workdays)	Major malfunction

12.4.2. In case there is an action that is not referred to in the section above (the table) it is necessary to specify the action and the maximum response time.

12.4.3. [IM] The Bidder shall specify the response times of the proposed service with relation to the maximum response times stated in the table in section 12.4. It is clarified that the bid must comply with the maximum response times, a bid that fails to meet these times will be disqualified.

12.4.4. [IM] Mechanism for transferring the data manually, for example by an encrypted email, will be available 365X7X24.

12.4.5. [IM] The Bidder will specify the service performance levels while operating under the assumption of approximately 300,000 users (the National Cyber Directorate is not committed to any number of users) and the guarantee of the Bidder to provide a response time to a DNS query that will not exceed 1mSec:

12.4.5.1. [IM] Number of possible DNS queries on average at a given time per hour and per day.

12.4.5.2. [IM] Number of possible DNS queries in peak time per hour.

12.4.5.3. [IM] Number of users that can be included in the service simultaneously and option to increase the number of the users and the time that is required, including a response to the number of queries in peak time per hour.

12.4.5.4. [IM] Estimate of the time for defining and integrating the service in the organization (estimated by 1,000 users, without a commitment by the National Cyber Directorate to the number of users in the organization) including a response to the definition of Block List and Allow List and handling False Positive.

12.4.5.5. [O] Other.

12.5. Usability reports

12.5.1. [IM] The service should allow end-to-end management and monitoring and inspection of the regularity of its operation (regularity of the communication DNS service).

12.5.2. [IM] The service should allow end-to-end management and monitoring and inspection of the regularity of the management interfaces, input processes of the intelligence feeds, lists update processes and more.

12.5.3. [IM] The service will provide capabilities for analyzing historic usage information and in real time (such as last time of use, frequency of use in the management portal and/or in API, number of logins to the management portal etc.).

12.5.4. [IM] The Bidder will provide key performance indicators (KPI) that the service will collect and store.

12.5.5. [O] The service will facilitate the definition of additional performance indicators, in addition to those set out in the previous section, by the user.

12.5.6. [O] The service will provide visual tools and viewing capabilities of the performance indicators as stated in the sections above in real time and historic data.

12.5.7. [O] The Bidder will specify in the report the False Positive level in time intervals (month, six months and one year).

12.6. Browsers and devices

12.6.1. [IM] The management interfaces should be based on WEB browsers as approved by the National Cyber Directorate (for example, browsers such as Chrome, Safari, Edge, Firefox).

12.6.2. [O] The service should be customized and supported by smartphones and tablets (Responsive) and allow comfortable viewing (for example, Android, iPhone, iPad).

12.6.3. [O] To the extent that the service allows access by an application installed in a mobile device, the Bidder is required to state this.

12.6.4. [O] The service should support future versions of standard mobile devices as long as the service is in use.

12.6.5. [O] The service should support future versions of browsers, as long as the service is in use.

12.7. Accessibility

12.7.1. [O] The service including its management interfaces should comply with the provisions set forth in the Equal Rights for People with Disabilities (Service Accessibility Adjustments) Regulations, 5773-2013 level AA according to the recommendation in the WCAG 2.0 Standard or, alternatively, comply with the ISO40500 Standard.

12.8. Service updates

12.8.1. [IM] The Bidder is required to ensure that the service that is provided to the National Cyber Directorate will be based on the official, full and latest version (General Availability).

12.8.2. [IM] The Bidder is required to ensure that the entire information that the users of the service inputted will be saved and will be available for the latest version that is currently in use.

12.8.3. [IM] The Bidder will ensure that the service updates that are performed will not harm, shut down or cause a change as a result of the information stored in the service.

12.8.4. [O] The Bidder will offer and will allow to the National Cyber Directorate to participate in the Beta versions of the service. The Directorate will decide whether or not to participate.

12.8.5. [IM] The Bidder will present to the National Cyber Directorate the RoadMap of the next versions at least once a year in coordination with the National Cyber Directorate.

12.9. Saving logs and documentation

12.9.1. [IM] For the avoidance of doubt, the logs of the service itself will include all the DNS queries and the answers that will be provided, whether or not the query was approved, blocked, changed, if a message stating that the domain does not exist or any other issue.

12.9.2. [IM] The Bidder will provide information regarding the saving of the logs of the service itself, as follows:

12.9.2.1. [O] Raw Data will be saved for a minimum period of six months.

12.9.2.2. [O] Notifications and reports will be saved for one year as a minimum.

12.9.2.3. [IM] The place and the manner that the information is saved and the manner it will be transferred to the National Cyber Directorate, on demand and in coordination with the National Cyber Directorate.

12.9.3. [IM] The Bidder will save the operational logs (for example, user management, permissions management and more) for a period of 3 months and will allow the transfer of this information to the National Cyber Directorate, during this period. The Bidder will specify where and in what manner the information is saved and how it will be transferred to the Directorate, on demand and in coordination with the National Cyber Directorate.

12.9.4. [IM] The Bidder will specify the implications stemming from the increase of the period of time for saving the documentation following the request made by the Directorate, with reference to time intervals of one year and a half, two years, two and a half years, and three years.

12.10. Survivability, backup, and recovery of data

12.10.1. [IM] The Bidder is required to specify the service survivability, backup, and recovery policy of the data of users, and shall refer to the protection service itself and to the management interfaces of the proposed service in the different levels, and shall refer to the

option of implementation (the service and the management interfaces) based on Anycast.

12.11. Training requirements

12.11.1. The Bidder is required to provide a regular training service to the National Cyber Directorate and to the managed organizations that implement the service within the framework of this Tender during the term of the engagement as stated in this section.

12.11.2. [IM] The Bidder shall provide frontal training sessions in the offices of the Directorate and in the offices of the organizations or by video conference.

12.11.3. [IM] The Bidder shall provide to the Directorate and to the managed organizations the entire materials that were presented in the training. If the training was provided by way of a video conference, the National Cyber Directorate and the organizations will receive a recording of the training. The Directorate and the organizations may use these materials for internal purposes for the purpose of training the service users

12.11.4. [IM] The training sessions that will be provided will be provided to the different levels of the service users.

12.11.4.1. Initial training, intended for the new users.

12.11.4.2. Advanced training designated for experienced users and that demonstrates advanced capabilities of the service.

12.11.4.3. Additional trainings, as may be required, such as: user management, work with API.

12.11.5. [IM] The training sessions will be provided at least twice a year regularly, and, to the extent that the Directorate and the managed organizations make such a demand in coordination with the Bidder – as a result of innovations, version updates, addition or change in the scopes of work and the service capabilities, changes in manpower in the National Cyber Directorate or in the managed

organizations, or for any other reason, at the request of the Directorate and/or the organizations.

12.11.6. [IM] Training sessions will be provided in English and/or Hebrew.

12.11.7. [IM] The instructors on behalf of the Bidder should have experience of at least 6 months in the proposed service and product, and experience in the subject matter of their training.

12.11.8. [IM] Training sessions will include full presentation of the service functionality such as: basic features, advanced features, block/allow policy settings, service definitions, interpretation of management interfaces display, understanding the information received from the service (D&I, logs and more).

12.12. User manuals

12.12.1. [IM] The Bidder will provide a user manual in English and/or in Hebrew by the service portal and its management interfaces.

12.12.2. [IM] The Bidder will provide on-line help screens in the service portal and in its management interfaces.

12.12.3. [O] To the extent that there are other options for user manuals in the proposed service, the Bidder should specify this.

12.12.4. [IM] The Bidder will provide an update of the new features that were added in the update version of the service (Release Notes) and will update the user manual accordingly.

12.13. Reference software

12.13.1. [O] The Bidder shall provide reference software in English and/or in Hebrew by the service portal and its management interfaces.

12.13.1.1. [O] The Bidder shall specify the technical requirements that the reference software complies with for the service, if any, with reference to the learning

management system (LMS) with a high integration scope worldwide and in the Israeli market, Hebrew and/or English support, compliance with the accessibility requirements in accordance with the Israeli law, including the ability to make accessible videos with subtitles, narration, assistive subtitles based on different visual impairments and more. See also the Equal Rights for People with Disabilities (Service Accessibility Adjustments) Regulations, 5773-2013 level AA according to the recommendations of the WCAG 2.0 Standard or, alternatively, the relevant page in the ISO40500 Standard, support of the ability to export and import content according to open standards such as SCORM, AICC and more.

12.13.1.2. [O] Support of standard browsers such as Edge, Chrome.

12.13.1.3. [O] Support of work with mobile phones such as Android, iPhone.

12.13.1.4. [O] Support of work with tablets, such as iPad, Microsoft Surface.

12.13.1.5. [O] Presentation of open test and closed test for the purpose of testing the competence level of users and awarding a score based on parameters that will be defined.

12.13.1.6. [O] Making accessible content for offline use.

12.13.1.7. [O] Tracking ability of the rate of progress in learning for each user.

12.13.1.8. [O] Ability to issue certificates to users who completed a study unit/course etc.

12.13.2. [O] The Bidder shall specify about the licensing model according to the specification

12.13.2.1. [O] The system will have the option to organizations in the market to integrate the content in their LMS systems, for no additional payment, in such manner that organizations will be able to monitor the progress in learning of their users.

12.13.2.2. [O] The license should allow exposure of the reference software and the content to internet users without limitation

12.13.2.3. [O] The National Cyber Directorate shall be the owner of the deliverables (such as content).

12.13.3. [O] The Bidder will specify the integration process and will refer to the following issues:

12.13.3.1. Update of the reference software content according to a functionality update in the portal and feedbacks received from the field – up to four times a year.

12.13.4. [O] The Bidder will specify the compliance of each content version of the reference software with the requirements of the National Cyber Directorate.

12.13.5. [O] The Bidder will specify the system of reference software solutions for the service, if any.

12.14. Integration of the service

12.14.1. [IM] The Bidder will specify the integration plan of the service among users in the Directorate and in the managed organizations for the service who connected within the framework of this Tender and will implement it upon commencement of the process (after the engagement takes effect) and after changing the versions and adding capabilities within the framework of the service.

12.14.2. [O] The Bidder will specify how it considers the Directorate as a strategic partner and how this will be manifested during the contractual engagement.

12.15. Current operation

12.15.1. [IM] The Bidder will specify the technical support provided to the users (that are part of different categories of users/different organizational levels) also with reference to technical capabilities within the framework of the service and also to actual support by service personnel (the dedicated integration and support team,

further information in section 10.3.2) in coordination with the National Cyber Directorate and the managed organizations that use the service:

12.15.1.1. [I] Means of communication of the users with the representatives on behalf of the Bidder:
- 12.15.1.1.1. [IM] Telephone
- 12.15.1.1.2. [IM] Email
- 12.15.1.1.3. [IM] Portal
- 12.15.1.1.4. [O] Other
- 12.15.1.1.5. [O] Specific means of communication for the National Cyber Directorate and the managed organizations within the framework of this Tender

12.15.1.2. [I] Support in the following cases:
- 12.15.1.2.1. [IM] A domain that was blocked for an unjustified reason (False Positive) as stated in section 12.4.1.
- 12.15.1.2.2. [IM] A domain that was not blocked and that ought to have been blocked (Miss Detection) as stated in section 12.4.1.
- 12.15.1.2.3. [IM] Malfunctions, as stated in the entire section 12.
- 12.15.1.2.4. [O] Other

13. Security requirements

13.1. Compliance with standards

13.1.1. [M] The Bidder is responsible for assuring that the proposed service is in compliance with the certification and standardization requirements laid down in the Tender (ISO27001 certification or CMMC DOD or SSAE SOC 2 and ISO27017/18) during the entire period of the Agreement. The Bidder's certification will include all components involved in the solution. It is necessary to attach to the bid a copy of the certification document.

13.1.2. [O] The Bidder is responsible for ensuring that the proposed service is in compliance with the certification and standardization requirements:
ISO/IEC 27701 in their latest version.
Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines during the entire term of the Agreement. The Bidder's certification will include all components involved in the solution. It is necessary to attach to the bid a copy of the certification document. If the Bidder has no existing certification, the Bidder is required to obtain such certification in one year as of the signing date of the Agreement.

13.1.3. [O] The Bidder is responsible for ensuring that the proposed service complies with the ISO 27032 certification and standardization requirements during the entire term of the Agreement. The Bidder's certification will include all components involved in the solution. The Bidder is required to attach to the bid a copy of the certification document. If the Bidder has no existing certification, the Bidder is required to obtain such certification in one year as of the signing date of the Agreement.

13.1.4. [O] The Bidder shall be responsible for assuring that the proposed service complies with the certification requirements of the certification method on behalf of the National Cyber Directorate. If the Bidder has no existing certification, the Bidder is required to

obtain such certification in one year as of the signing date of the Agreement.

13.1.5. [M] The Bidder shall be responsible for ensuring that the service provider in the country on its behalf complies with the certification standardization requirements during the entire term of the Agreement. The Bidder's certification will include all components involved in the solution. The Bidder is required to attach a copy of the certification document. If the Bidder has no existing certification, the Bidder is required to obtain such certification in one year as of the signing date of the Agreement.

13.1.6. [O] The Bidder will specify compliance with additional international standards such as FEDRAMP, CSA STAR, and will indicate the rank/hierarchy level in the certification requirements.

13.2. General – Data protection

13.2.1. [M] The proposed service is required to implement a data protection policy. The Bidder is required to attach an information document or a policy document that includes the following:

13.2.1.1. [M] Description of the architecture of the interfaces service/system.

13.2.1.2. [M] Controls of data security that are used by the service/system starting from the physical level of the protection of the service/system.

13.2.1.3. [M] Distribution of the data security responsibilities (Shared responsibility module) between the manufacturer and the tenant.

13.2.1.4. [M] Manner of identification and response to incidents.

13.2.1.5. [M] Assessment of employees and reliability tests.

13.2.1.6. [M] Detection of vulnerabilities and installation of patches.

13.3. Implementation of mechanisms

13.3.1. The service will include the following mechanisms and the Bidder will specify the implementation of the mechanisms:

13.3.1.1. [M] Two-stage identification process (MFA).

13.3.1.2. [M] Permissions management.

13.3.1.3. [M] Information regarding the implementation of the management of Session Timeout (disconnection after no user interaction within a predetermined amount of time).

13.3.1.4. [M] Encryption of data at rest and in motion.

13.3.1.5. [M] Monitoring and logs existing in the service/system.

13.3.2. [M] In any event in which the Bidder uses the computer infrastructure of another vendor, the Bidder is required to specify this or attach a document describing how the Bidder shares the responsibility with the infrastructure provider and what measures the Bidder applies for the purpose of protecting the information from the vendor and from harm to the infrastructure.

13.4. Saving and erasure of data

13.4.1. [M] The Bidder is required to protect the information that it stores in accordance with the provisions of the Israeli Protection of Privacy Law (Protection of Privacy Law 5741-1981) and the Protection of Privacy Regulations (Data Security) 5777-2017 and the requirements laid down in the Tender. The Bidder will specify whether the protection includes threats analysis, evaluation of risks and setting of controls for the purpose of handling risk.

13.4.2. [M] The Bidder will specify or attach a document describing the geographic location where the data will be saved.

13.4.3. [M] The Bidder will specify how and in what manner the saving of the data is in compliance with the Israeli privacy law (Protection of Privacy Law 5741-1981) and the Protection of Privacy Regulations (Data Security) 5777-2017 regarding the storage of personal data.

13.4.4. [M] The Bidder will specify what types of controls are implemented for the purpose of ensuring that the data is not transferred to other geographic regions.

13.4.5. [M] The Bidder will specify whether it can, after the end of the service or on demand, erase the data of the Directorate from its systems, without the ability to recover the data – including metadata, and anything else related to the data of the Directorate and the users. The Bidder will specify how this erasure is performed and what approvals are granted for the purpose of this matter.

13.5. Compliance and periodic tests

13.5.1. [M] The Bidder will specify the regulations and the certifications of the service and will make available to the Directorate the certification documents.

13.5.2. [M] The Bidder will specify the manner of implementation and frequency during the entire term of engagement of periodic data security tests of the type penetration tests and Vulnerability assessment tests that include the following, among other:

13.5.2.1. [M] Tests for the infrastructure on which the service/system operate.

13.5.2.2. [M] Applicative tests.

13.5.2.3. [O] Social Engineering tests and/or employee awareness training.

13.6. [O] Physical and environmental security

The Bidder shall specify the manner of securing the facilities from which the service is operated (for example, principal facility, backup facilities and more) that includes reference to the following issues as a minimum:

13.6.1. In the event that the user uses third-party vendors (such as a cloud provider) the Bidder is required to provide information also about this data.

13.6.2. The Bidder will specify if and in whether manner the facility protection includes a response to physical and environmental security threats including nature-based and human-based events, including malfunctions.

13.6.3. The Bidder will specify the existing environmental security policy including control and enforcement processes.

13.6.4. The Bidder will specify the compliance of the facilities with customary standards, such as TIA942.

13.7. [O] Employee reliability

13.7.1. The Bidder will specify whether there is and what is the policy regarding response to internal threats, including protection of the service/system against employees who were unreliable and/or subcontractors who maintain the service.

13.7.2. The Bidder will specify whether and in what frequency the Bidder performs background tests and screening tests for employees in the organization, the logic access control to servers, and whether there is a separation between different roles and work environments. The Bidder will provide such information in compliance with the customary standards in the market.

13.8. Protecting the supply chain

13.8.1. [M] The Bidder will specify the manner of management of the threats in connection with the engagement with its subcontractors, and perform risk analysis of its supply chain.

13.8.2. [O] The Bidder will specify the material subcontractors that constitute a major part of the service and whether the tenant's data is transferred to these subcontractors.

13.8.3. [M] The Bidder will describe how it handles threats in the supply chain of the service.

13.9. Application data security

13.9.1. [M] The Bidder will specify whether the proposed service was developed, with emphasis on information security and privacy considerations.

13.9.2. [M] The Bidder will specify whether the proposed service was developed in compliance with the SDLC Standard (Security development life cycle) that is customary in the market and whether it includes an assessment of the application risks (Threat modeling), whether the developers were trained on data security, and whether tests such as Static/Dynamic analysis are implemented, including periodic performance of penetration tests.

13.9.3. [M] The Bidder is required to specify the protection mechanisms of the applicative interfaces (different types of API).

13.9.3.1. [O] The service will enable protection of the management interfaces by a firewall system (WAF – Web Application Firewall) based on the Allow List.

13.9.4. [O] The Bidder will specify whether it is necessary to provide a specific review of the implementation of the security mechanisms, for example, whether mTLS was used and what is the actual implementation method.

13.10. Data security operation

13.10.1. [M] The Bidder is required to operate regularly the data security in the service/system, this operation will include current risk management of all components that are used for the operation of the service, starting from the physical protection of the facility.

13.10.2. [M] The Bidder will operate the service/system regularly, that will include:

13.10.2.1. The performance of identification actions of data security incidents and response.

13.10.2.2. Response to data security incidents.

13.10.2.3. Current monitoring of the service/system for detection of malfunctions and incidents.

13.11. Support channels

13.11.1. [M] The Bidder will specify the existence of protections of the support channels for the service/system as stated in this Tender, that

will prevent abuse of the said channels by unauthorized users, including the existence of the following:

13.11.1.1. Strict procedures regarding the manner of identification of the tenants receiving the service/system.

13.11.1.2. Procedures regarding the conditions required for the performance of a change in the service or access to the data of the Directorate.

13.11.1.3. Controls, monitoring and test samples/periodic tests of the implementation of procedures.

13.11.2. [M] The Bidder will specify how it intends to identify the Directorate personnel when using these service channels and what actions the Bidder performs for the purpose of preventing a manipulation of support services in favor of the cyber-attacks.

13.12. Incident management

13.12.1. [M] The Bidder is required to specify its ability to detect data security incidents in the service, warn the tenants receiving the service/system at the earliest opportunity and act for the purpose of handling the incident while observing the customary standards in the market.

13.12.2. [M] The Bidder, as part of the incident management process, is required to keep for a period of six months, the entire relevant information, including log files, actions that were performed in the service/system, response scenarios and system states for future analysis.

14. Separation plan and erasure of data

14.1. The Bidder shall specify the separation and on-the-job training plan that the Bidder proposes to perform with the Directorate and with the entity that the Directorate will designate as its substitute upon termination of the engagement, to the extent that such a substitute is selected. After the implementation of the separation plan, the Bidder is required to erase and remove from its systems the entire information that the Directorate and the organizations that connected within the framework of this Tender uploaded to the service during the term of engagement. For the avoidance of doubt, the said undertaking will also apply to information that the vendor received within the framework of the pilot, to the extent that a pilot was held. The Bidder shall respond to the following aspects, among other, within the framework of its response:

14.1.1. Schedules for the implementation of the separation and on-the-job training, that will not exceed a period of three months in total.

14.1.2. Manner of transfer, from the Bidder to the Directorate and to the other organizations, of the entire data that the Directorate and the organizations that connected to the service uploaded within the framework of this Tender during the term of engagement, including: Block List, Allow List, intelligence feeds, optimization of the data that was performed in the service offered by the Bidder, permanent reports (if defined), encryption keys, data tables and any other item of information that is required for the purpose of reading data and using such data in the systems of the Directorate or anyone acting on its behalf.

14.1.3. Third-party software products, to the extent required, for the purpose of performing the migration of the data from the Bidder's systems to the systems of the Office or anyone acting on its behalf and to the extent that these are required.

14.1.4. If IP addresses and domains that are the property of the National Cyber Directorate were used, the Bidder shall return them to the National Cyber Directorate upon completion of the service.

Chapter C – The bid booklet that will be submitted by the Bidders

0. Instructions regarding the response of the Bidder to the Tender

0.1. This chapter constitutes the Bidder's response to the Tender. The Bidder is not required to respond to any other part at this stage.

0.2. Bidders are required to follow closely the instructions set out in this chapter so that the bid can be properly evaluated. Bidders are prohibited from adding or changing any of the terms set forth in the Tender.

0.3. In any event of questions or ambiguity in the Tender documents, the Bidder is required to deliver to the Directorate clarification questions, as stated in chapter A of the Tender documents. When submitting a bid within the framework of the Tender, the Bidder accepts the Tender terms and conditions and the Bidder shall be precluded from raising any claims to the Directorate regarding the said terms and conditions.

0.4. Unless otherwise stated expressly, the Bidder may add information and details in addition to those required in the bid specification appendix. Lack of information or information that fails to satisfy the demand might result in a low score of the bid or its disqualification, at the sole discretion of the Directorate. Bidders are referred to the said in Appendix 9 regarding the information that is required in the sections that are marked as required sections ("M"]).

0.5. The bid in the Tender shall be in effect for a period of 10 months, starting from the bid submission deadline. The Directorate shall be entitled to announce the extension of the effect of the bid for additional periods of three months, until a final decision is made, and until a Bidder is elected as the winning bidder in the Tender. The Bidder may not withdraw from its bid during the said periods.

1. Instructions regarding the manner of submitting the response

1.1. The response shall be submitted in a sealed envelope, without an indication of the Bidder information or any other identifying information. The Bidder will write only the number and the name of the Bidder on the envelope.

1.2. The Bidder will attach to the exterior part of the envelope an additional envelope, sealed, without any information about the Bidder's details or any other identifying information, that will include the name of the Bidder and the information of the contact persons on behalf of the Bidder (telephone number and address) for the purpose of returning the response, if required.

1.3. In addition to a printed response, the envelope will include two identical copies of the response (including declarations, approvals, and appendixes, as required) and a USB flash drive, that will include the relevant documents of the response in open format (doc or docx only) and the appendixes of the response (including declarations, approvals, and appendixes, as required) signed and scanned as PDF. The copies that will be attached and the response files will be identical to the first printed and signed copy. The USB will not include additional files, in addition to the files of the Tender as stated in this section.

1.4. In the event of a non-conformity between the signed response and the copies that are attached or saved in the USB that was attached, the signed response shall take precedence.

1.5. The person submitting the response on behalf of the Bidder will leave the premises of the Directorate immediately after submitting the response, without waiting and without any delay. If a person submitting the response is in the premises of the Directorate after submitting the response, the Office may, at its sole discretion, disqualify the response of the Bidder in limine.

1.6. It is emphasized that Bidders may not submit their response by postal mail or registered mail, fax or email. These responses will not be presented to the Tender Committee and will be disqualified in limine.

1.7. Bidders should note that there are security procedures at the entrance to the Directorate building that include inspection of personal documentation, and that there is a parking problem in the area that might cause a delay at the entrance to

the building. Bidders are required to take this into consideration for the purpose of ensuring timely arrival to the tender box.

1.8. The response will be submitted in Hebrew and/or in English only, together with all the bid documents (including declarations, approvals and appendixes, as required). The authorized signatory(s) on behalf of the Bidder will affix their full signature and the stamp of the corporation anywhere in the Tender documents where this is required expressly. It is clarified that in any event the Hebrew version of the requirements laid down in the Tender shall take precedence. It is possible to sign with the signature and the stamp as said on the copy that will be submitted as the first copy and photocopy it in the two identical copies.

1.9. If the Directorate published an updated version of the Tender or Appendixes thereof following clarifications that it received, the Bidder is required to assure that the response will be submitted according to the latest version.

2. Information regarding the Bidder

2.1. Information regarding the Bidder in the Tender

1. **Bidder's name** (as written in the relevant register)	
2. **Type of incorporation** (for example – a limited liability company/private company etc.)	
3. **Bidder place of incorporation** – state the country where the incorporation is registered.	
4. **Registration date**	
5. **Identification number** (for example, C.N)	
6. **Information regarding activities in Israel** (in the event of an Israeli corporation, the bidder should not fill this part)	State whether the corporation is registered in Israel as a foreign company – Registration no. – Registration date –
	Name of representation in Israel (if any):
	Type of representation (for example, limited liability company):
	ID. No. (for example, C.N):
	Date of establishment of the local branch:
7. **Contact person on behalf of the bidder for the purpose of participating in the Tender**	Name:
	Tel.:
	Email:

2.2. Information regarding the manufacturer:

(Relevant in the event that the manufacturer is an authorized reseller)

1. **Name of the proposed service(s)** To the extent that there is more than one service, it is necessary to specify all names of the proposed services)	
2. **Name of manufacturer** (as registered in the relevant register)	
3. **Region abroad where the service is operated** (if the service was not yet operated in the Israeli region)	
4. **Type of incorporation** (For example, limited liability company/private company etc.)	
5. **Manufacturer place of incorporation -** state the country where the incorporation is registered	
6. **Manufacturer ID. No.** (For example, C.N)	

3. Proof of compliance with the Threshold Conditions

3.1. In accordance with the provisions set forth in this chapter, the Bidder shall specify its compliance with the Threshold Conditions set out in the Tender. Only a Bidder who satisfies the entire Threshold Conditions set out hereunder may participate in the Tender.

3.2. ☐ By checking X in this section, the Bidder declares and undertakes that it satisfies the entire Threshold Conditions set out in chapter A of the Tender documents, as follows:

3.2.1. **Administrative Threshold Conditions**

3.2.1.1. The Bidder is a corporation lawfully registered in Israel or abroad.

3.2.1.2. The Bidder does not hold and is not held by another Bidder in the Tender (holding for the purpose of this matter – holding directly or indirectly of 25% or more of the means of control, as meant by this term in the Securities Law 5728-1968), and another entity does not hold 25% or more in two bidders. In addition, the Bidder is not a subcontractor of another Bidder in the Tender in connection with the performance of the services in this Tender.

3.2.1.3. The Bidder keeps its books of account and records that it is obligated to keep in accordance with the provisions of the Income Tax Ordinance [New Version] and the Value Added Tax Law 5736-1975 (hereinafter: the "VAT Law") or the Bidder is exempt from keeping them.

3.2.1.4. The Bidder reports to the Assessing Officer regarding its income and reports to the Director regarding transactions that are chargeable with tax, in accordance with the provisions of the VAT Law.

3.2.1.5. No convictions: the Bidder and "interested party" to the Bidder (as meant by this term in section 2B of the Transactions with Public Bodies Law) were not convicted of more than two offenses in accordance with the provisions of the Foreign Workers Law 5751-1991 and the Minimum Wage Law 5747-1987 or were convicted as said, however at least one

year since the date of the last conviction and until the submission date of the bid lapsed.

3.2.1.6. Proper representation: the Bidder complies with the provisions of section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 or that the provisions of the said law do not apply to the Bidder, and acts in accordance with the provisions set forth in section 2B1 of the Transactions with Public Bodies Law.

3.2.1.7. **Obligation to engage in industrial cooperation** – the Bidder undertakes to perform all actions that are required for the purpose of maintaining industrial cooperation in accordance with the provisions of Mandatory Tender Regulations (Mandatory Industrial Cooperation) 5767-2007 (hereinafter: the "**Industrial Cooperation Regulations**"), in the event that the provisions of these Regulations apply as part of the competitive procedures that will be conducted by virtue of the Tender.

3.2.2. **Professional Threshold Conditions**

3.2.2.1. The Bidder is the manufacturer of the product/system/proposed service and is the right holder therein; alternatively, the Bidder is required to be a licensed reseller on behalf of the manufacturer of the product/system/the proposed service.

3.2.2.2. The service passed within the framework of this Tender will be a cloud-based service (SaaS)[2].

3.2.2.3. The Bidder has experience in the last 3 years in the supply of the proposed product/service within the framework of the response to this Tender in the following minimum scopes:

3.2.2.3.1. The product was supplied/the service was provided to at least 75 organizations (of the governmental or public or private sector).

3.2.2.3.2. Out of the organizations enumerated in section 3.2.2.3.1, at least 10 organizations have 5,000 users per organization and at least 1,500 queries per day for each user.

[2] The Bidder is required to take account of the fact that the service should be a cloud-based service (SaaS) in accordance with the policy of the Government as stated in resolution 231 of the Government dated August 1, 2021.

3.2.2.3.3. Out of the organizations enumerated in section 3.2.2.3.1, at least 45 organizations have 3,000 users per organization and at least 1,500 queries per day for each user.

3.2.2.3.4. Out of the organizations enumerated in section 3.2.2.3.1, 20 organizations have at least 100 users per organization and at least 1,500 queries per day for each user.

3.2.2.4. For each of the 75 organizations enumerated in section 3.2.2.3.1, the Bidder performed integration and provided dedicated support by a dedicated team of employees that were trained for the purpose of this matter, over the period of one year as a minimum (in the years 2019-2023).

It is clarified that compliance with this Threshold Condition may also be proven by a vendor/subcontractor with whom the Bidder maintained/maintains a dedicated engagement for the purpose of this matter.

The Bidder is required to state whether the vendor/subcontractor complies with this condition as stated above.

3.2.3. The Bidder is required to present experience under the definition/update of the block policy in at least 5 organizations, out of the list of organizations enumerated in sections 3.2.2.3.2 – 3.2.2.3.4 that receive the service.

The definition of the block policy shall be manifested also by the fact that the Bidder can incorporate intelligence feeds from different sources and/or in different formats, including the ability to include the information that is provided by an external entity.

4. Additional undertakings of the Bidder

4.1. Declarations of the Bidder at the time of submitting the response

4.1.1. The Bidder read carefully the Tender documents, its Appendixes, conditions and parts, including the entire clarifications that were published by the Directorate, understood their entire content and agrees to their content.

4.1.2. The Bidder read carefully the terms of engagement with the winning bidder, and in this regard the Agreement including Appendixes thereof, understood their content and agrees to their content.

4.1.3. As of the date of submitting this affidavit, the Bidder is not under bankruptcy or liquidation proceedings and no material lawsuits the Bidder that might impair its performance, to the extent that the Bidder wins the Tender, are conducted against it.

4.1.4. There is no impediment under any law preventing the participation of the Bidder in the Tender and, to the best of the Bidder's knowledge, there is no conflict of interests, whether directly or indirectly, whether professional and whether in connection with the Bidder's business, and the Directorate, and in any event that any concern regarding the existence of such a conflict of interests arises, the Bidder shall be obligated to notify the Directorate forthwith about the same and take immediate measures to eliminate such conflict of interests as said.

4.1.5. The submission of the bid in the Tender or the performance of the engagement subject matter of the Tender by the Bidder shall not give rise to a conflict of interests, whether directly or indirectly, between the Bidder and the Client or the Tender Holder.

4.1.6. The Bidder undertakes to notify the Tender Holder in writing, without delay, regarding any material change that occurred in the information that the Bidder provided within the framework of its bid in the Tender.

4.1.7. This response is submitted in good faith

4.2. No collusion in the Tender

4.2.1. The information contained in this bid is provided independently by the Bidder at its discretion, without any consultation, arrangement, or connection with another Bidder.

4.2.2. The particulars of the bid were not presented or will be presented to any person or corporation that submits bids in this Tender.

4.2.3. The Bidder was not involved in any attempt to induce another bidder not to submit bids in this Tender, and was not involved in any manner in a bid that was submitted by another Bidder.

4.2.4. The Bidder was not and does not intend to be involved in an attempt to induce another Bidder to submit a bid that is higher or lower than its bid;

4.2.5. The Bidder was not involved in an attempt to induce another bidder to submit a bid that is uncompetitive in any manner.

4.2.6. The Bidder undertakes to notify the Directorate regarding any change in any of the particulars as stated above from the time the Bidder signs the affidavit and until the bids submission date.

4.3. Property rights

4.3.1. The Bidder is the owner of the proposed service in its bid. The Bidder shall be entitled, under any law and/or agreement, to sell the service and the products that the Bidder offers in the Tender, and this shall not constitute any violation of any third-party property rights.

4.4. Independent Bidder

4.4.1. The Bidder does not hold or is held by another Bidder in the Tender (holding for the purpose of this matter – holding directly or indirectly, as defined in the Securities Law 5728-1968) in 25% or more of the means of control.

4.4.2. Another entity does not hold 25% or more of the means of control in the Bidder and in another Bidder in the Tender.

4.4.3. The Bidder is not a subcontractor on behalf of another Bidder in the Tender, in connection with the performance of the services in this Tender.

4.5. Business controlled by a woman

4.5.1. A Bidder that is a "business controlled by a woman" and who is interested to have priority for the purpose of this matter, will attach a confirmation and an affidavit to its bid, and all in accordance with the provisions of section 2B of the Mandatory Tender Law.

5. Parts in the bid that the Bidder asks to keep classified

Check X where appropriate:

5.1. ☐ By checking X in this section 5.1 the Bidder declares that its bid does not include parts that the Bidder wishes to keep classified.

5.2. ☐ By checking X in this section 5.2 the Bidder declares that its bid includes parts that it wishes to keep classified.

5.3. In accordance with the provisions set forth in Chapter A of the Tender documents, the following are the pages, the sections or the documents contained in the bid that the Bidder wishes to withhold their inspection from other Bidders (on the grounds of exposure of a trade secret or a professional secret or any other reason as stated in Regulation 21(E) of the Mandatory Tender Regulations).

Page/section number	**Section subject matter**	**Reason for preventing the exposure**

6. By affixing our signature hereunder, we confirm the following:

6.1. We read the entire instructions set forth in the Tender, we understand and accept each section of the Tender, and the Bidder shall be precluded and estopped from raising any claim against the conditions set forth in the Tender from the time of submitting its bid.

6.2. The particulars contained in this bid including Appendixes thereof are true and the Bidder is capable and intends to provide everything stated in its bid and the instructions set forth in the Tender.

6.3. Our bid is submitted in accordance with the terms set forth in the Tender and it complies with the conditions and the requirements laid down in the Tender.

6.4. We are authorized to sign and undertake in this bid in the name of the Bidder.

Date	Name	Signature and stamp of the authorized signatory
Date	Name	Signature and stamp of the authorized signatory
Date	Name	Signature and stamp of the authorized signatory

Confirmation of attorney

I, the undersigned, _____, Adv. confirm that the aforenamed signatories who signed this bid in the Tender jointly/severally are the lawful authorized signatories for the Bidder _____ in this Tender.

_____	_____	_____
Date	License No.	Signature and Stamp

List of Appendixes that will be attached to the bid

Appendix no.	Appendix title	Appendix description
Appendix 1	Company extract/Certificate of Proper Management (To be attached by the Bidder (no wording exists in the Tender documents)	A valid extract containing the information about a company or partnership issued by the Corporations Authority; can be produced online in the internet website of the Corporations Authority (by clicking the link "produce company extract") showing that the company does not owe annual fee debts for the years that preceded the year in which the bid is submitted. With regard to a company, the Tender Committee will inspect that the company is not a company in violation of the law or that the company received notification that it is about to be registered as a company in violation of the law. A Bidder that is an association will attach a Certificate of Proper Management. A Bidder that is a cooperative, will attach a certificate of cooperative registration from the Registrar of Cooperative Societies.
Appendix 2	Certificate regarding management of books of account and records	A valid certificate from an "authorized official" in accordance with the provisions of the Transactions with Public Bodies Law, from an accountant or a tax advisor, confirming the

		management of books of account, and reporting to the tax authorities as required by law. The document can be downloaded from the internet website of the Tax Authority.
Appendix 3	Affidavit regarding no convictions in respect of the employment of foreign workers and minimum wages	The Bidder is required to fill in the affidavit attached as Appendix 3.
Appendix 4	Affidavit regarding the employment of persons with disabilities	The Bidder is required to fill in the affidavit attached as Appendix 4.
Appendix 5	Response regarding proof of compliance with the professional Threshold Conditions	The Bidder is required to attach an Appendix in which the Bidder will specify how it satisfies the requirements laid down in section 4.2 in Chapter A of the Tender documents, the Appendix should include information regarding the process and the means that are included in the service. The Bidder is required to attach screenshots and reports for the purpose of proving its compliance with the conditions.
Appendix 6	Form for the submission of a joining application of a vendor to the suppliers database under certification level B of the National Cyber Directorate	The Bidder is required to fill in the affidavit attached as Appendix 6.
Appendix 7	Declaration of the manufacturer regarding compliance with the NIMBUS data security requirements	The Bidder is required to fill in the affidavit attached as Appendix 7.
Appendix 8	Price bid	The Bidder is required to submit the price bid according to the instructions set forth in the Tender documents.
Appendix 9	Bid specification	The Bidder is required to provide in this Appendix a

		detailed response to all the demands that were stated with relation to each of the services offered by the Bidder.
Appendix 10	Bid Guarantee	
Appendix 11	Q&A document signed by the Bidder. To be attached by the Bidder	The Bidder is required to attach the Q&A document as stated in section 2.3.6 of this Tender, signed by the Bidder.
Appendix 12	Agreement for the Pilot Stage To be attached by the Bidder	The Bidder is required to attach the Agreement for the Pilot Stage attached in Chapter D of the Tender documents, signed according to the requirements made from the Bidder.
Appendix 13	Agreement To be attached by the Bidder	The Bidder is required to attach the Agreement attached in Chapter E of the Tender documents, signed according to the requirements by the Bidder.
Appendix 14	Service price list	The Bidder is required to attach a link to the overseas price list of the service. If the overseas price list is not public, the Bidder is required to attach it as an appendix to the bid.

Appendix 1 – Company extract/Certificate of Proper Management

A valid extract containing the information about a company or partnership issued by the Corporations Authority that can be produced online in the internet website of the Corporations Authority (by clicking the link "produce company extract"), showing that the company does not owe annual fee debts for the years that preceded the year in which the bid is submitted. With regard to a company, the Tender Committee will confirm that the company is not a company in violation of the law or that the company received notification that it is about to be registered as a company in violation of the law.

A Bidder that is an association will attach a Certificate of Proper Management.

A Bidder that is a cooperative will attach a certificate of registration for a cooperative, issued by the Registrar of Cooperative Societies.

Appendix 2 - Certificate regarding management of books of account and records

A valid certificate from an "authorized official" in accordance with the provisions of the Transactions with Public Bodies Law, from an accountant or a tax advisor, confirming the management of books of account, and reporting to the tax authorities as required by law.

The document can be downloaded from the internet website of the Tax Authority.

Appendix 3 - Affidavit regarding no convictions in respect of the employment of foreign workers and minimum wages

I, the undersigned, _____, ID. No._____, having been warned to tell the truth or else I shall be subjected to penal action as set forth by law hereby declare the following:

I submit this affidavit in the name of _____ who is the bidder (hereinafter: the "**Bidder**") who wishes to engage in connection with Public Tender no. 1-1.2024 - "TAFNIT" (PDNS) - Services for the denial of access to malicious domains and redirection enforcement option, for the National Cyber Directorate. I declare that I am authorized to submit this affidavit in the name of the Bidder

In this affidavit the term "**interested party**" shall have a meaning assigned thereto in the Transactions with Public Bodies Law 5736-1976 (hereinafter: the '**Transactions with Public Bodies Law**'). I confirm that I received an explanation regarding the meaning of this term and that I understand this term.

The term "**offense**" shall mean – an offense pursuant to the provisions of the Foreign Workers Law (Prohibition on Unlawful Employment and Assurance of Fair Conditions) 5751-1991 or in accordance with the provisions of the Minimum Wage Law 5747-1987, and regarding transactions for the purpose of receiving a service, as defined in section 2 of the Law for Increased Enforcement of Labor Laws, 5772-2011, also an offense in violation of the provisions set forth in the Third Schedule of the said law.

(Check X where appropriate).

☐ The Bidder and interested party thereof **were not convicted** of more than two offenses until the last date for submission of bids (hereinafter: the "**Submission Date**") in Contract no. _____ for the supply of _____ for _____.

☐ The Bidder or interested party thereof **were convicted** in a judgment of more than two offenses, and at least **one year passed** as of the date of the last conviction and until the Submission Date.

☐ The Bidder or interested party thereof **were convicted** in a judgment of more than two offenses, and **one year** as of the date of the last conviction and until the Submission Date **did not pass**.

I affirm that this is my name and signature and the content of my affidavit is true.

_____	_____	_____
Date	Name	Signature and Stamp

Confirmation of attorney

I, the undersigned, _____ Adv., confirm that on _____ Mr./Mrs. _____ who identified himself/herself by ID. No. _____/whom I know in person, appeared before me, in my office in _____ St. in the town/city of _____ and after I warned him/her that he/she is required to declare the truth, and that his/her failure to do so shall subject him/her to statutory penalties, he/she confirmed the truthfulness of this Affidavit and signed it in my presence.

_____	_____	_____
Date	License No.	Signature and Stamp

Appendix 4 – Affidavit regarding the employment of persons with disabilities

Queries to the Director-General of the Ministry of Labor, Social Affairs and Social Services as required under this affidavit shall be delivered by the Headquarters for the Inclusion of Persons with Disabilities in the Labor Market in the following email: mateth.shiluv@economy.gov.il
For questions you may contact the employers support center, in the following email: info@mtlm.org.il/**Tel.: 1700-507-676**

I, the undersigned, _____, ID. No._____, having been warned to tell the truth or else I shall be subjected to penal action as set forth by law hereby declare the following:

I submit this affidavit in the name of _____, the bidder (hereinafter: the "**Bidder**") who wishes to enter into an agreement in connection with Public Tender no. 1-1.2024 - "TAFNIT" (PDNS) - Services for the denial of access to malicious domains and redirection enforcement option, for the National Cyber Directorate. I declare that I am authorized to submit this affidavit on behalf of the Bidder.

Check X where appropriate:

☐ The provisions of section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 **do not apply** to the Bidder.

☐ The provisions of section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 **apply** to the Bidder and the Bidder observes them.

In the event that the provisions of section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 (hereinafter: the "Equal Rights Law") **apply to the Bidder**, check X where appropriate:

☐ The Bidder employs less than 100 employees.

☐ The Bidder employs 100 employees or more.

In the event that the bidder employs 100 employees or more, check X where appropriate:

☐ The Bidder undertakes that to the extent that it wins the Tender, it will contact the Director-General of the Ministry of Labor, Social Affairs and Social Services for the purpose of inspecting the performance of its obligations pursuant to section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 and, if necessary – for the purpose of receiving instructions in connection with their implementation.

☐ The Bidder undertook in the past to request from the Director-General of the Ministry of Labor, Social Affairs and Social Services to conduct an inspection of the performance of its obligations pursuant to section 9 of the Equal Rights for Persons with Disabilities Law, made such a request from the Director-General as said and if the Bidder received instructions for the purpose of performing its obligations, **it took action for the purpose of performing such obligations** (in the event the Bidder undertook in the past to contact the Director-General and a contract was made with the Bidder in respect of which the Bidder made such undertaking as said).

The Bidder undertakes to deliver a copy of the affidavit it submitted in accordance with this paragraph to the Director-General of the Ministry of Labor, Social Affairs and Social Services in 30 days as of the date of the contract.

Name	Date	Signature

Appendix 5 – Proof regarding compliance with the professional Threshold Conditions

1. **<u>The Bidder has experience in the last 3 years as a minimum in the supply of the proposed product/service within the framework of the response to this Tender, in the following minimum scopes:</u>**
   - 1.1. The product was supplied/the service was provided to at least 75 organizations (of the governmental or public or private sector).
   - 1.2. Out of the organizations enumerated in section 1.1 above, at least 10 organizations include 5,000 users per organization and at least 1,500 queries per day for each user.
   - 1.3. Out of the organizations enumerated in section 1.1 above, at least 45 organizations include 3,000 users per organization and at least 1,500 queries per day for each user.
   - 1.4. Out of the organizations enumerated in section 1.1 above, at least 20 organizations include 100 users per organization and at least 1,500 queries per day for each user.

Name of organization (The Bidder is required to specify the names of paying and active organizations only, as of the bid submission date. In circumstances in which it is not possible to state the name of the organization, it is necessary to specify the information to the extent possible regarding the sector and the sphere of activity)	**The supplied product/the service that is provided to the organization** (name of the system, service model)	**Sector** (Specify whether the organization is from the governmental, public or the private sector)	**Number of users in the organization** (To the extent that there are different types of users – specify this) [It is possible to specify the number of users in increments of 10]	**Number of queries per day for each user in the organization** (to the extent that there are different types of queries, specify this) [It is possible to specify the number of users in increments of 10]	**Duration of the performance of the service by years** (specify the start date and the end date)	**Representati behalf of t customer fo purpose receiving recommend** (It is necessa state at leas recommend customer

2. <u>For each of the 75 organizations as stated in section 1.1 above, the Bidder performed integration and provided dedicated support by a dedicated team of workers that were trained for the purpose of this matter, over a period of one year as a minimum (in the years 2019-2023).</u>

It is clarified that compliance with this Threshold Condition can also be proven by a vendor/subcontractor with which the Bidder had/has a special contract with for the purpose of this matter. The Bidder is required to specify whether the vendor/subcontractor as stated above satisfy this condition.

No.	**Name of organization** (The Bidder is required to specify the names of paying and active organizations only, as of the bid submission date. In circumstances in which it is not possible to state the name of the	**Integration process performed in the organization** (Specify the key elements in the process)	**Support service that is provided to the organization** (Specify the nature and the manner of the support service that is provided to the organization)	**Team of workers** (Specify the dedicated team that provides the support, including its training)	**State whether the vendor/subcontractor as stated above satisfy this condition** (If your answer is yes, specify)	**Period of performance of the service in years** (Specify start date and end date)	**Representative on behalf of the customer for the purpose of receiving a recommendation** (It is necessary to state at least 2 recommending customers)

	organization, it is necessary to specify the information to the extent possible regarding the sector and the sphere of activity)						
1.							
2.							
3.							
4.							
5.							

3. <u>The Bidder is required to present experience in the definition/update of the block policy in at least 5 organizations, out of the list of the organizations as stated in sections 1.2-1.4 above, to which the service is provided.</u>

The definition of the block policy will also be manifested by the ability of the Bidder to integrate intelligence feeds from different sources and/or in different formats, including the ability to include information that is provided by an external entity.

No.	**Name of organization** (The Bidder is required to specify the names of paying and active organizations only, as of the bid submission date. In circumstances in which it is not possible to state the name of the organization, it is necessary to specify the information to the extent possible regarding the sector and the sphere of activity)	**Process and features of the definition/update of the block policy** (Specify the key elements in the process and the features)	**Duration of the performance of the services in years** (Specify start date and end date)	**Representative on behalf of the customer for the purpose of receiving a recommendation** (It is necessary to state at least 2 recommending customers)

1.				
2.				
3.				
4.				
5.				

Appendix 6 – Application form by a vendor to join the vendors database under Certification B of the National Cyber Directorate

(Duly made affidavit, to be filled by the authorized signatory on behalf of the vendor)

I, the undersigned, _____, ID. No._____, having been warned to tell the truth or else I shall be subjected to penal action as set forth by law hereby declare the following:

I, the undersigned, _____ ID. No. _____ acting in the position of _____ submit this affidavit in the name of _____, that is the bidder (hereinafter: the "**Bidder**") who wishes to engage with the Tender Holder in Public Tender no. 1-1.2024 - "TAFNIT" (PDNS) - Services for the denial of access to malicious domains and redirection enforcement option. I declare that I am authorized to submit this affidavit in the name of the Bidder.

I hereby submit this application for the inclusion of the vendor as a vendor who declared under self-assessment (B) and who filled the vendors questionnaire for the strengthening of the supply chain of the National Cyber Directorate in version _____ under certification level B.

Name of the process to which the declaration applies _____ as a vendor under risk level _____ for the following types of engagement:

☒ System-wide requirements
☐ Software development
☒ Cloud-based system
☐ Remote access
☐ OT security
☒ Website hosting

☐ I read Appendix 3 – "Information regarding the filling of Appendixes 1+2" and accordingly I filled this application form. I request that the information regarding the vendor will be published by the National Cyber Directorate in the Directorate website, in a page that will contain the information regarding the vendors who

declared under self-assessment B that they filled the vendors questionnaire for the strengthening of the supply chain of the National Cyber Directorate.

☐ The undersigned is aware that the information posted in the website will not include the response of the vendor to the strengthening questionnaire and that anyone interested in inspecting or viewing the answers of the vendor to the questionnaire will make direct contact, according to the contact information provided below.

☐ The undersigned is aware that to the extent that the Directorate receives queries stating that the vendor does not provide to the interested persons the full report containing the answers to the questionnaire and/or the questionnaire and the necessary proof, as the case may be, and that the mere filling of the questionnaire by the vendor in self-assessment and/or the proof, as the case may be, are questionable, the Directorate shall be entitled to remove the information of the vendor from the main vendors database of the Directorate at its sole discretion.

☐ The undersigned is aware that it undertakes that it complies with the supply chain methodology of the National Cyber Directorate based on the information provided above.

☐ The undersigned is aware that the publication in the website will include the name of the supplier Pvt. Co. No./License Dealer No., the types of engagements that the vendors declared in the system, ranking of the vendor's risk level, whether the vendor was examined by a certified vendors examiner, the system that was used for the purpose of performing the examination, the name of the process that under examination, the questionnaire version, name of the contact person with an indication of the certificate date of validity, and together with the additional following data (according to my choice). Check X for the information you decide will be published in the website:

I affirm that this is my name and signature and the content of my affidavit is true.

Vendor telephone number: _____ official vendor email: _____
Name of officer: _____ ID. No. _____ Tel.: _____
Email: _____ Date: _____ Signature: _____

Confirmation of attorney

I, the undersigned, _____, Adv. confirm that on _____ there appeared before me in my office in _____ St. in the city/town of _____ Mr./Mrs. _____ who identified himself/herself by ID. No. _____ whom I know in person, after I warned him/her that he/she is required to declare the truth, and that his/her failure to do so shall subject him/her to statutory penalties, he/she confirmed the truthfulness of this Affidavit and signed it in my presence.

_____	_____	_____
Date	License No.	Signature and Stamp

Appendix 7 – Declaration by manufacturer regarding compliance with the NIMBUS data security requirements

Manufacturer's statement

This Commitment can be signed in Hebrew or in English

To:
[Israel National Cyber Directorate]

To:
The Government Procurement Administration

Re: **Engagement with [Israel National Cyber Directorate] (hereinafter: the "Customer") for the supply of [Name of Service] (hereinafter: the "Service")**

1. I, the undersigned. _____, hold the position of _____ in _____, which owns the intellectual property of the following service(s) (hereinafter: the "Manufacturer"):

1. Sequence no.	2. Name of the service for which this appendix has been submitted
3. 1	4.

(Rows may be added if necessary)

2. The service is offered by (mark one of the options):

☐	Our company (the Manufacturer) or our subsidiary in Israel
☐	Other company that is certified by us to offer and supply the services listed above. Specify the name of the Company _____(hereinafter: the "**Reseller**")

3. If the service is offered by the Manufacturer, it undertakes that it holds the full rights to sell the service, to undertake to the requirements detailed in Appendices C1 [Information Processing for Services in Software as a Service (SaaS) Configuration] and D1 [Security and Cyber for Services in Software as a Service (SaaS) Configuration] of Chapter 3 of Central Tender 01-2022 for the Addition of Services to the Government Cloud Marketplace, in its updated edition that is published on the **שגיאה! ההפניה להיפר- קישור אינה חוקית.** (hereinafter: the "Tender"), and sections 4.2-4.6 hereinafter.

4. If the service is offered by the Reseller, I declare and undertake as follows:

   4.1. The Reseller holds the full rights to sell the service, and to commit to the requirements detailed in Appendices C1 [**Information Processing for services in**

software as a service (SaaS) configuration] and D1 [**Security and Cyber for Services in Software as a Service (SaaS) Configuration**] on Chapter 3 of the Tender.

4.2. The terms of use of the service will be the terms of use specified in section 3.10.5 of the tender, with the exclusion of section 3.10.5.4.

4.3. The service will be deployed in the Israeli Region no later than September 30, 2024, or in 12 months from the date the Israeli Region was operated by the cloud provider, whichever is later (hereinafter: "Service Deployment Date in the Israeli Region").

4.4. Until the Service Deployment Date in the Israeli Region, the service may be provided from the Overseas Region or from the largest region of the cloud provider in the EU from which the service is provided. All in accordance with the provisions of section 3.6.3.2 of the tender documents, with the necessary changes.

4.5. Upon deployment of the service in the Israeli region, the manufacturer/reseller (as applicable) will assist in transferring the accounts and data to the Israeli Region without any change in user accounts, with the exception of automatic re-association in the Israeli Region, including order balances, other obligations, credits etc. Prior to providing the service in the Israeli region, the manufacturer/reseller must prepare for the transfer of the service as mentioned in this section, including assisting in building the service so the transfer costs which will be imposed on the customer will be minimal.

4.6. The service will meet the requirements mentioned in sections 3.6.3.3 and 3.6.4 of the tender documents.

4.7. Manufacturer's Approval:

Manufacturer name: _____

The role of the signatory with the Manufacturer: CFO

Date: _____ Signature and stamp: _____

4.8. Reseller's Approval (If the service is offered by the reseller):

Reseller name: _____

The role of the signatory with the Reseller: _____

Date: _____ Signature and stamp: _____

Appendix 8 – Price bid

The price bid that forms the price **Pi** as stated in section 5.5 of the Tender.

At the time of submitting the bid in this Tender, the Bidders will deliver a price bid that will be submitted concurrently with the Bidder in a sealed and separate envelope, on which the Tender number, the words "price bid" and the Bidder's name will be written. The price bid will include two parts, according to the following format:

Information regarding the components

Component	**Price bid for component in ILS (excluding VAT)**	**Percentage of the fixed discount from the official price list of the manufacturer that is given as part of the bid (B)**	**Price after discount**
Fixed monthly cost for the management and maintenance of the service **(A)**		Do not fill	Do not fill
Price of an annual license of use of the official price list prices of the manufacturer **(P)**			

The price proposed by the Bidder will be in new Israeli shekels, or in a foreign currency out of the following foreign currencies: U.S. dollar, euro, pound sterling, **and will not include VAT**. For the avoidance of doubt, it is clarified that to the extent that VAT applies to the payment, the Directorate shall pay the VAT as required by law at the time of paying the consideration in accordance with the Agreement.

For the avoidance of doubt, it is clarified that the Directorate is not obligated to purchase any minimum number of users and/or hours.

The price will include all services related to this Tender, including API that is not limited by the number of calls (API calls) and that allows the usage of all the system capabilities including technical support, operational support, training, SLA and any other service

related and that is required for the purpose of receiving the services in accordance with the Tender.

Appendix 9 – Bid specification

1. **Manner of answering the bid specification appendix**

1.1. The bid specification appendix specifies the quality requirements from the proposed service.

1.2. The Bidder is required to specify for each of the sections that are marked as "M" or "IM" or "O":

1.2.1. The level of support of the service in the requirements laid down in the section: satisfies the requirement, partially satisfies the requirement, does not satisfy the requirement.

1.2.2. Full information and explanation regarding the manner that the response answers the requirements laid down in the section.

A section that will only include a reference to the support level without information might be awarded the minimum score for this section, and this could result in the disqualification of the bid, in the event of a section marked as "M".

1.3. In the detailed bid the Bidder is required to maintain the numbering of the sections in Appendix 9 (for example – section 4.2.3 in the bid will include information regarding the compliance of the bid with the requirement of section 4.2.3 in the bid specification appendix). A response or an appendix without an indication of its relation to a specific section might not be evaluated, at the discretion of the Office.

1.4. Documents regarding sales or appendixes that are not related directly to the response provided under this Tender may not be submitted. The Directorate will not respond in the evaluation score to the additions exceeding the requirements laid down in this Tender. The submission of irrelevant documents and that impede the evaluation of the bid might result in its disqualification, at the discretion of the Tender Committee.

1.5. It is emphasized that no answer, an answer that fails to answer the requirement, lack of answer to the requirement, or an unclear and

ambiguous answer might result in a low score of the bid or its disqualification at the sole discretion of the Directorate, and taking into consideration the type of the requirement as stated in sub-section E hereunder.

1.6. The Tender sections are classified and marked as follows:

Mandatory, marked as "M"	A section that the Bidder is obligated to comply with in a minimum level for the required service is also known as a mandatory section (the "mandatory" element is explained in the content of the section, and not by the mere need to answer. The need to answer applies to all sections of the Tender, except for sections that are marked as "I" as explained in section D below). In these sections the Bidder is required to declare that it satisfies the requirement described in the section and describe how the Bidder satisfies this requirement. In addition to the need to satisfy the requirement **fully**, the response to the section will be scored according to the quality of satisfaction with the requirement, in the manner as stated in the response that will be submitted. Lack of an answer, an answer that does not fully satisfy the requirement, or an unclear and unambiguous answer in this type of section might result in disqualification of the bid, at the sole discretion of the Tender Committee.
Important, marked as "IM"	A quality section. The Bidder's bid in these sections will be scored according to the capabilities that will be stated in its answer to these sections, as evaluated based on the scoring criteria that were defined in advance. The weight of these sections is higher than the quality sections that are marked as "O".

	In these sections the Bidder is required to declare that it satisfies the requirement described in the section and describe how it satisfies this requirement (even if this is partial satisfaction of the requirement). The answers to this section will be scored according to the quality of compliance with the requirement as stated in the answer that will be submitted. No answer, an answer that does not answer the requirement or an unclear and unambiguous answer in this type of section might result in a low score for that section, and consequently in the disqualification of the bid, at the sole discretion of the Tender Committee and as stated in section 5.1 of the Tender documents.
Option, marks as "O"	Quality section. The Bidder's bid in these sections will be scored according to the capabilities that will be stated in its answer to these sections, as evaluated according to the scoring criteria that were defined in advance. No answer, an answer that does not answer the requirement, or an unclear and ambiguous answer in this type of section might result in zero score in that section.
Information, marked as "I"	Sections that are intended to provide general information about the service, the requirements for the service or guidelines regarding the required answers. These sections, in and of themselves, do not affect the quality score, and the Bidders should not answer them within the framework of the bid. There could be sub-sections of "I" section that are marked as "M" or "O", as the case may be, and for which the Bidder is obligated to give an answer accordingly, in accordance with the instructions set forth in this section above.

Appendix 10 – Bid Guarantee

Name of Bank/Insurance Company: _____
Tel.: _____
Fax: _____

Re: Non-linked Guarantee

To
The Government of Israel
By the National Cyber Directorate
Guarantee no. _____

We hereby guarantee towards you for the payment of any amount, up to the amount of ILS 1,500,000 (one million and five hundred thousand new Israeli shekels) that you will demand from: _____ (hereinafter: the "Debtor") in connection with Public Tender no. 1-1.2024 - "TAFNIT" (PDNS) - Services for the denial of access to malicious domains and redirection enforcement option.
We will pay you the aforesaid amount in 15 days as of the date of your first demand that was delivered to us in a letter in registered mail or in person, and you shall not be obligated to give reasons for your demand and without raising any claim of defense against you that the Debtor may have in connection with the obligation towards you, or demand first the settlement of the said amount from the Debtor.
This Guarantee shall be in effect until August 14, 2024.

A demand made under this Guarantee shall be referred to the branch of the bank/insurance company in the address _____

_____
Name of the Bank/Insurance Company

_____
Bank no. and branch no.

_____
Address of the branch of the bank/insurance company

This Guarantee is nontransferable and non-assignable

Date	Full Name	Signature and Stamp

Appendix 11 – Q&A Document signed by the Bidder

Appendix 12 – Agreement for the pilot Stage signed by Bidder

Appendix 13 – Agreement signed by the Bidder

Appendix 14 – Service price list

Chapter D – Agreement for the Pilot Period

Agreement for the Pilot Stage

Entered into and executed in _____ as of this ___ day of _____ 202_

Between: The Government of Israel in the name of the State of Israel
By the National Cyber Directorate in the Prime Minister's Office
10 HaBarzel St., Tel Aviv
(Hereinafter: the "**Directorate**")

The first party;

And between: _____
Address _____
(Hereinafter: the "**Vendor**")

The second party;

Whereas: The Directorate wishes to purchase a cloud-based service (SaaS) for the purpose of providing services preventing access to malicious domains and the option to enforce redirection to an approved server (the "**Services**");

And whereas: For the purpose of receiving the Services, the Tender Holder published Public Tender no. 1-1.2024 - "TAFNIT" (PDNS) - Services for the denial of access to malicious domains and option to enforce redirection to an approved server (the "**Tender**");

And whereas: The Vendor submitted a bid in the Tender and passed to the stage of the evaluation of the proof of concept of its bid (the "**Pilot**") and the Vendor is ready to perform the Pilot in accordance with the conditions set forth in the Tender and in this Agreement;

Now, Therefore, it is Declared, Stipulated and Agreed between the Parties as Follows:

1. General

1.1. The following Appendixes are attached to this Agreement:

1.1.1. **Appendix A** – The Tender and the file containing the clarification questions and answers;

1.1.2. **Appendix B** – The Vendor's bid as submitted within the framework of the Tender;

1.1.3. **Appendix C** – Processing data for Services in a format of software as a service (SaaS);

1.1.4. **Appendix D** – Confidentiality Statement;

The preamble to this Agreement and Appendixes thereof constitute an integral part hereof.

1.2. The terms used in this Agreement shall have the meaning ascribed thereto in the Tender unless defined expressly in the Agreement. This Agreement shall be construed in a manner that will maintain the requirements laid down in the Tender, both express and implied, and the purpose of the Tender for the supply of the equipment and the Services to the Directorate in an optimal manner.

1.3. In the event of discrepancy between this Agreement and any other provision relating to the Service (such as licensing agreement, use agreement, End User License Agreement) in a manner that cannot be resolved in accordance with the rules of interpretation set out above, the provisions of the Agreement shall take precedence.

2. Terms of use of the Services

2.1.1. The Directorate shall be entitled to make any use of the Service within the framework of the performance of its roles and its purpose as a public service for the State of Israel and its citizens, subject to the provisions of the law applicable to it. In addition to the provisions set forth in this section, there shall be no limitation of any kind, including rules of "permitted use" in the Vendor's Service.

2.1.2. Any information of security value that will be produced as a result of the use of the Services and the products of the Vendor within the framework of the Pilot performed under this Agreement will be shared with other entities and organizations, with or without information from other sources of the Directorate, according to the requirements of the Directorate and its procedures within the framework of the performance of its duties. Notifications of the Directorate that are made public in the information distribution channels of the Directorate may also include raw data from the Service.

2.1.3. Notwithstanding the aforesaid, a client or anyone acting on its behalf shall not use the Services for the following purposes:

2.1.3.1. Use for commercial purposes such as resale.

2.1.3.2. Infringement of the intellectual property rights of the Vendor including the performance of reverse engineering.

2.1.4. There shall be no limitation on behalf of the Vendor on the types of the systems and the information that the clients may migrate to the Service including critical systems with high sensitivity.

2.1.5. There shall be no limitation preventing from the clients to transfer content data, including the logic that was defined by the client to another entity, including a cloud provider or another service.

3. Manner of performing the Pilot

3.1. The Pilot shall be performed in accordance with the provisions set forth in the Tender.

3.2. The Vendor shall perform the Pilot under the management of the Israeli contact person that was presented in its bid to the Directorate.

3.3. For the purpose of performing the Pilot, the Vendor shall be obligated to provide to Directorate at least six licenses under different profiles for full use in the proposed system. In addition, the Vendor is required to make available to the Directorate at least one managed organizations' manager license.

3.4. The Pilot shall be performed on the system in its version as presented in the bid to the Tender, in such manner that will facilitate the full use of the Service, including the production of reports.

3.5. Prior to the commencement of the Pilot the Vendor shall provide training regarding the use of the system to the Pilot users on behalf of the Directorate. The training shall be provided by a video conference on the date that will be set by the Directorate for the purpose of this matter.

3.6. The Pilot shall be managed by the Directorate. The instructions of the Directorate shall take precedence in any question relating to the present performance of the Pilot.

3.7. In any event in which the Vendor wishes to make changes in the Pilot, the Vendor shall deliver a reasoned request for the purpose of this matter. The decision of the Directorate for the purpose of this matter shall be final.

3.8. To the extent that the Vendor provides a service to the Directorate as stated in section 3.3 of the Tender documents, the Pilot shall be performed in accordance with the terms of the Tender and this Agreement, irrespective of the existing service that will continue in accordance with the terms applicable to it. Accordingly, the Vendor shall provide to the Directorate user licenses and service for the Pilot period in accordance with this Agreement, concurrently with the continuation of the performance of the existing service.

4. The Pilot period

4.1. The Pilot period shall commence on the date defined by the Directorate and that shall not exceed 45 days (the "**Pilot Period**").

4.2. The Directorate shall be entitled to shorten the Pilot Period in the event that the Directorate finds, at its sole discretion, that there is no purpose in continuing the Pilot with the Vendor (for example: fast success or, alternatively, material failure) or in the event there is an operational need or any other need that requires the shortening of the Period.

4.3. The Directorate shall be entitled to cancel the Pilot stage at its sole discretion.

5. Consideration

5.1. The Pilot shall be performed for no consideration of any kind, including reimbursement of expenses or any other payment.

6. Termination of the engagement

6.1. Without derogating from the provisions set forth in this Agreement, and in particular in section 4.2 therein, the Directorate shall be entitled to terminate

this Agreement forthwith upon the occurrence of any of the following events:

6.1.1. If the Vendor discontinued conducting its business for a consecutive period exceeding 30 days; it is clarified that in such circumstances as said the Vendor shall be obligated to notify the Directorate immediately after the cessation of its operations.

6.1.2. If a provisional, interim, or permanent liquidator is appointed for the Vendor; and it is clarified that upon the occurrence of the events described above the Vendor shall notify the Directorate immediately about such an appointment as said.

6.1.3. If a temporary or a permanent receiver is appointed for the business conducted by the Vendor and/or for the property of the Vendor; and it is clarified, upon the occurrence of the events described above, the Vendor shall be obligated to notify the Directorate forthwith regarding such an appointment as said.

6.1.4. If an order for stay of proceedings is issued against the Vendor. And it is clarified, upon the occurrence of the events as stated above, the Vendor shall be obligated to notify the Directorate forthwith regarding the issuance of such an order as said.

7. Undertakings and declarations of the Vendor

7.1. The Vendor declares that it read the entire terms and requirements laid down in the Tender, understood them and the Vendor undertakes to observe the entire terms and requirements of the Tender, the bid and this Agreement, accurately, efficiently, expertly and skillfully.

7.2. The Vendor hereby declares that it possesses the experience, competence, know-how, tools, equipment, inventory and manpower that are required for the purpose of performing the Pilot successfully, and the Vendor shall endeavor to the best of its ability to make the Pilot successful.

7.3. The Vendor declares and undertakes that its actions, including its products, the Services and the software tools that will be operated within the framework of the Pilot exist and are implemented in accordance with the

provisions of the Israeli law and statutes, and that the software, the products, or any other action of the company within the framework of the Pilot do not and shall not constitute any violation of the law, including, but not limited to, intellectual property laws, computer laws and protection of privacy laws.

7.4. The Vendor declares and undertakes that there is no impediment under any law prohibiting the engagement with the Vendor in this Agreement.

8. Supervision

8.1. The Vendor shall permit to the Directorate or anyone acting on its behalf to supervise the performance of the requested Services, their nature and quality, for the purpose of inspecting and supervising the manner that the Vendor performs its undertakings (except for data storage facilities of a third party).

8.2. During the performance of the Pilot, and for the purpose of supervising and controlling its performance, the Vendor shall provide to the professional team on behalf of the Directorate any information or report that is demanded by them and that are relevant for the purpose of providing the Services according to the opinion of the professional team, on the date and in the manner prescribed by them;

9. Confidentiality, security provisions and conflict of interests

9.1. Information for the purpose of this section shall mean any information that was inputted by the users in the Service during the Pilot (including queries and searches and intelligence information inputted in the Service), information containing details of the Vendor's users, or the details regarding the use that the Directorate makes with the Service, and any information related to the Pilot or to the Tender specification.

9.2. The Vendor hereby declares that it is aware that the information to which the Vendor will be exposed during the Pilot in accordance with this Agreement has special sensitivity, and the Vendor undertakes that it and anyone acting on its behalf shall keep the information in strict confidence and shall not make any use of the said information, except for the performance of the Services within the framework of the Pilot in accordance with the Tender and this Agreement. For the avoidance of doubt, and without prejudice to the generality of the foregoing, the Vendor undertakes that it

and anyone acting on its behalf shall not publish, transfer, notify, communicate, or disclose to any person the information, except for information that is in the public domain, or information whose provision is mandatory by law. Failure to perform this undertaking might constitute an offense pursuant to Chapter G (National Security, Foreign Relations, and Official Secrets) of the Penal Law 5737-1977.

9.3. The Vendor undertakes to sign each of the workers that the Vendor will employ in the performance of the Services to the Directorate within the framework of the Pilot performed under this Agreement, including its Bidders and anyone exposed to the information related to the Pilot, on the Confidentiality Statement, in the form attached as Appendix D of this Agreement.

9.4. The Vendor undertakes not to make any publication in connection with the Directorate, the Tender, or the performance of the Pilot, without obtaining the prior and written approval of the Directorate.

9.5. The obligation of the Vendor regarding the information shall apply as long as the Vendor possesses the information, even after the expiration of the term of engagement.

9.6. The Vendor undertakes to observe the entire instructions of the Directorate and the Security Division in the Directorate, including in anything related to the classification of information, handling information and security clearance. The Vendor undertakes to cooperate, to the extent required, in any inspection that will be required for the purpose of this matter.

9.7. The Directorate undertakes not to disclose the Vendor's work methods to a third party other than the employees of the Directorate or consultants employed by the Directorate, that shall also be bound by the duty of confidentiality. For the avoidance of doubt, and notwithstanding the aforesaid, to the extent that any competent court orders on the disclosure of a specific particular as stated above, the Directorate shall observe the instructions of the competent court.

9.8. 30 days after the completion of the Pilot, the Vendor shall erase fully the entire copies of the Pilot data from its systems or from the Services

environment in the manner that will not enable their recovery, unless the Directorate requested not to act in such manner.

9.9. The Vendor declares and undertakes that the performance of the Pilot shall not give rise to any conflict of interests, whether directly or indirectly, between the Vendor and the Directorate, and that in any event that any concern about a conflict of interests arises, the Vendor shall notify the Directorate about the said, without delay, and shall take immediate measures to eliminate the said conflict of interests.
The position of the Directorate shall be decisive in any event of a concern about a conflict of interests.

10. Cyber incident

10.1. In any event of a cyber-attack or a suspected cyber-attack on the Vendor's systems that are used or that the related to the Services that the Vendor provides to the Directorate, and that might affect the data security of the Directorate, as defined in section 9 of the Agreement, the Vendor shall report to the Directorate promptly and no later than 12 hours as of the time of becoming aware of the attack or the suspected attack, together with the full relevant information that the Vendor knows about the attack, and that might affect the data security of the Directorate, as defined in section 9 of the Agreement, the steps that are taken by the Vendor for the purpose of handling the attack, and the information that was exposed and/or that might be exposed as a result of the attack.

10.2. The Vendor shall report and shall update the Directorate during the response to the attack according to the demands made by the Directorate, and shall cooperate with the requirements made by the Directorate in anything related to the information that was exposed and/or that might be exposed as a result of the attack.

11. Relationship between the parties

The parties hereby declare and agree as follows:

11.1. The relationship between the parties under this Agreement is the relationship between a tender holder and a contractor executing orders only, and shall not give rise to employer-employee relationship between the

Directorate and Vendor's employees or the subcontractors on its behalf, with all ensuing consequences.

11.2. Without derogating from the provisions of section 11.1, it is clarified that the Directorate shall not make any payment to the National Insurance Institute and all other social-benefit payments in connection with the persons employed by the Vendor.

12. Remedies in consequence of a breach

12.1. If the Vendor found that there is a probable opportunity that it will not be able to satisfy perform its undertakings, in whole or in part, for any reason, or that the Vendor will not be able to meet the dates and the terms of the Pilot, the Vendor shall notify immediately about the said verbally and by email to the Directorate.

12.2. The provisions of this section shall not derogate from the right of the Directorate to seek any other relief in accordance with this Agreement or in accordance with any law in respect of the breach.

13. Liability for damages

13.1.1. The Vendor shall be held liable for any harm, damage or loss of any kind caused to the client, its employees and anyone acting on its behalf and to any entity, person or any other third party, in consequence of an act or omission of the Vendor, its employees, agents, subcontractors or anyone acting in its name and in its place as part of the performance of this Agreement, up to the liability limit set out in section 13.1.5.

13.1.2. The client, anyone acting on its behalf or employed by the client shall not be held liable and shall not incur any payment, expense, harm, loss, or damage in respect of any harm, damage or loss of any kind caused to the Vendor, anyone acting on its behalf or anyone employed by the Vendor. The aforesaid shall not apply to damage that was caused maliciously or as a result of gross negligence and for which the client is held liable by law.

13.1.3. The termination of this Agreement shall not derogate from the liability of the Vendor for damages whose cause of action arises out

of this Agreement or from the performance of the Services under this Agreement or in connection therewith.

13.1.4. The Vendor undertakes to pay and indemnify the client fully, to the extent that the organization is obligated to make payment in a peremptory judgment given by a competent court and whose execution was not suspended, to pay any amount in respect of any financial obligation that the Vendor owes in accordance with this Agreement, whether stemming from a claim of an employee of the Vendor or anyone acting on behalf of the Vendor (including subcontractors) or an employee of the client or a third party, or of an insurer or from any other source, up to the liability limit set out in section 13.1.5.

13.1.5. Unless otherwise stated expressly in this Agreement, the liability limit of the Vendor for the payment of damages or indemnity to the client for any damage event shall not exceed the amount of the damage that was caused or the indemnity that is required and up to two times of the scope of actual consumption of the Services from the Vendor by all clients during the Pilot Period, whichever is lower, and with the addition of the entire expenses of the client, including legal expenses and attorney fees that the Vendor shall incur in connection with a suit brought in connection therewith, and with the addition of linkage differentials and statutory interest. The limitation of liability as said shall not apply to the following: damage caused deliberately to a third party by an act or omission of the Vendor, its employees or anyone acting on its behalf; damage covered under the insurances that the Vendor undertook to take out in accordance with this Agreement; damage to tangible property or damage that constitutes personal injury, death, sickness, physical, mental or intellectual impairment; damage caused as a result of breach of the duty of confidentiality.

13.1.6. The client shall notify the Vendor regarding any claim or demand made under this section at the earliest opportunity after its receipt, and shall afford to the Vendor an opportunity to defend against it. In such circumstances as said, the client shall not agree to the claims that were made or held against the Vendor, and for which the Vendor is held liable in accordance with this Agreement, without obtaining the prior and written approval of the Vendor, and

shall notify to the Vendor in advance regarding its intention to settle with the plaintiff.

14. Modification

Any modification of the provisions set forth in this Agreement shall be executed in advance and in writing with the approval of both parties hereto.

15. Miscellaneous

15.1. Any notice in accordance with this Agreement shall be transmitted by email and shall be deemed to have reached its recipient 24 hours after its transmission, unless there is an indication suggesting that the transmission of the document failed.

15.1.1. The official email address of the Directorate is: mailto:cyber-michrazim@cyber.gov.il;

15.1.2. The official email address of the Vendor is: _____;

15.2. The parties submit to the sole and exclusive jurisdiction of the competent courts in the district of Tel Aviv (the place of residence of the Tender Committee on behalf of the Directorate) in anything related to and arising out of this Agreement. This Agreement shall be governed by the laws of the State of Israel.

15.3. This Agreement, jointly with the provisions set forth in the Tender, exhausts everything agreed between the parties hereto and any agreement or arrangement that were made prior to and until the signing of this Agreement shall be null and void.

And in witness hereof the parties are hereby undersigned:

The Directorate	**The Vendor**

Appendix C – Data processing

1. Protected data

1.1. Without derogating from the obligations of the Vendor in any other place, the Vendor shall be responsible for guarding, protecting and maintaining the integrity of the protected data in its systems and the Vendor shall not access this data, shall not permit another to access this data, shall not make any use or change in this data and shall not permit any use or change, whether by way of an act and whether by way of an omission, that is not permitted under the provisions of the Israeli law and in accordance with the provisions set forth in the Agreement and this Appendix.

1.2. The Vendor shall be responsible for ensuring that the clients and the users will have regular access to the protected data, in accordance with its obligations set out in this Agreement, and in any event the Vendor shall not deny from them access to the said data, in a manner that is in contradiction to the provisions of the Agreement or the Israeli law.

1.3. The Vendor understands that the protected data includes information regarding the work processes of the Government of Israel and data that is partly related to the citizens and the residents of the State of Israel. Accordingly, any exposure, harm, damage, denial of access, loss of protected data or exposure of data to a third party that might cause to the Tender Holder, to the clients and the users, and to other third parties, serious losses, and shall be obligated to protected the protected data according to the highest standards existing in the market, and not transfer it to any third party in accordance with the provisions set forth in this Appendix.

1.4. Protected data shall not be kept in a public cloud infrastructure other than a cloud infrastructure of one of the cloud providers who won the cloud tender.

1.5. The obligations of the Vendor with relation to the protected data shall apply as long as the data is stored in its systems, even after expiration of the term of engagement.

1.6. The Vendor shall permit the storage and full documentation of any access and use made by the client and its users to the different Services.

1.7. The Vendor shall have the option to save the documentation for a period of at least one year in such manner that it will be available continuously to the client and to the tender holder.

2. Content data

2.1. The clients shall be entitled to produce content data in the Vendor's systems or by the Vendor's systems, and migrate to the Vendor's systems in the cloud any content data that the clients will deem as necessary, subject to the provisions set forth in any law, including content data under different sensitivity levels, including content data of clients that are subject to different limitations by operation of the law, and the Vendor shall have no claim and shall not impose any limitation in connection therewith.

2.2. In accordance with the Israeli law applicable to the content data of some of the clients as updated from time to time, there are requirements with respect to the protection of the data against its disruption, alteration, or unauthorized exposure. The laws that apply to the data include, *inter alia*, the Security in Public Bodies Law, 5758-1998, the Commercial Torts Law, the State Property Law, and specific laws governing the operations of the State and the civil servants in different areas. The obligations with relation to the protected data under any law are imposed solely on the clients, who are the owners of the data, and not on the Vendor, however only and unless otherwise stated expressly in the Tender documents. The Vendor is obligated to make any reasonable effort for the purpose of allowing the clients and the Tender Holder to meet the different obligations applicable to them under any law with relation to such protected data as said. The provisions of this section shall not derogate from any obligation applicable to the Vendor under any law.

3. Use of the protected data

3.1. The Tender Holder and the clients are the exclusive owners of the protected data and the Vendor shall be deemed as the processor of the protected data and the Vendor shall not make any action in the protected data including storage and saving of the data, its processing and transfer to any third party, however only in accordance with the provisions of the governing law in the State of Israel and in accordance with the following instructions:

3.1.1. For content data – with the client's approval, according to a digital instruction, and for the regular supply of the services that were purchased.

3.1.2. For processing data – in the required minimal level for the normal supply of the services that are purchased within the framework of the Agreement, including improvement of the cyber protection of the Vendor's systems or the Services, the amounts charged in respect whereof and the performance of the obligations of the Vendor in accordance with the Agreement. It is emphasized that the use of the processing data for the purpose of improving the Vendor's Services that is not part of the improvement of the said Services for the clients, *inter alia*, is prohibited, unless the Tender Holder grants its written approval in connection therewith.

3.1.3. For subscription data – in the required minimum level for the regular supply of the Services that are purchased within the framework of the Agreement, the amounts charged in respect whereof and the performance of the obligations of the Vendor in accordance with the Agreement.

3.2. Without derogating from the foregoing, the Vendor undertakes to keep the data for the periods of time as stated hereunder:

3.2.1. Content data – a minimum of 12 months. The data will be kept for a longer period only after the provisions set forth in section 1.12.1.1 have been fulfilled.

3.2.2. Processing data and subscription data – 90 days, unless the client gives a digital instruction to extend this period of time.

3.3. Without derogating from the foregoing, and for the avoidance of doubt, the Vendor will not sell, lease, or perform any other commercial transaction in the protected data, and in this regard will not transfer the data to another after processing, transferring, or selling the data as part of the data of other users after the erasure of identifying information, or in any other constellation, without obtaining the prior and written approval of the Tender Holder.

3.4. The Vendor shall not store protected data in its systems in contravention of the provisions set forth in the Agreement and in this Appendix, and in accordance with a digital instruction, and will ensure that such data that is stored in its systems will be disposed, in accordance with the provisions set forth in any law.

3.5. Without derogating from the obligations of the Vendor, the Vendor shall apply the necessary precautions for the purpose of ensuring that the access to protected data is granted only to authorized entities on behalf of the Vendor that require such access to the data for the purpose of providing the Services to the clients. The Vendor is required to ensure that the exposure and the use of the protected data to the authorized entities shall be in the minimal level required for the purpose of providing the service regularly, and according to the obligations imposed on the Vendor. The Vendor shall train the authorized entities regarding the purposes of the use of the data, and the obligations imposed on them in accordance with the law and the provisions set forth in this Agreement as a result of the exposure to such data.

3.6. Erasure of protected data

3.6.1. In 30 days as of the date of receiving the client's request, or in 90 days as of the termination date of the engagement, for any reason, the SaaS service provider shall deliver to the client the entire data of the client, unless the client announced that it was not interested in the data. To the extent that the service allows the client to recover data or erase it directly, the Vendor shall permit the client to perform the said action in 30 days as of the expiration date of the engagement and the Vendor shall provide reasonable technical assistance in the recovery of the data and its erasure and will present to the client proof that the entire data was indeed recovered or erased as required. The entire data shall be recovered in a standard, updated and non-proprietary format.

3.6.2. 90 days after the expiration date of the engagement, or according to a digital instruction demanding the erasure of data and according to the terms of the service, the Vendor shall erase fully the entire copies of the content data in its systems or in the Services environments in a manner that will not enable their recovery, unless otherwise stated in this Agreement.

3.6.3. Further to the aforesaid, and subject to its obligations under any law, the Vendor shall erase from its records and databases any processing data and subscription data that are not necessary for the purpose of performing the actions permitted under this section.

4. Confidentiality

4.1. The parties agree that the protected data is confidential and may not be used contrary to the provisions of the Agreement, or transferred to any other entity without obtaining the prior and written approval of the Tender Holder.

4.2. The Vendor undertakes to keep in confidence security tools including encryption tools such as stamps and encryption keys that the Vendor provides to the client, and not to provide to any other party any tools or technological assistance in decoding the security tools without obtaining the prior and written approval of the Tender Holder.

4.3. Without derogating from the foregoing, the Vendor shall be obligated to apply all measures required from it for the purpose of keeping in confidence the subscription data and the processing data that are saved in the Vendor's systems in a confidential and secure manner, and in this regard the Vendor undertakes that:

4.3.1. This data shall be protected by the most advanced technological measures existing in the market (state-of-the-art).

4.3.2. Access to these data by the employees of the Vendor shall be made only by authorized persons who require such access and only in the required minimal scope.

4.4. The Vendor shall be held liable for ensuring that secondary processors on its behalf who will receive from the Vendor access to protected data for the performance of the Services to the clients shall be bound by the confidentiality obligation set out in this Appendix and in any event the Vendor shall be held solely liable for any of their violations of this obligation.

5. Privacy

5.1. Without derogating from its obligations in Appendix E and in the Agreement, the Vendor undertakes to act in accordance with the provisions of the Protection of Privacy Law 5741-1981 (hereinafter: the "Protection of Privacy Law") and the regulations enacted thereunder, and any other legislation under Israeli law in connection with privacy under Israeli law for the purpose of enabling the clients to upload personal data that is subject to the relevant legislation (hereinafter: "Personal Data") to the cloud. For the purpose of this matter, it is emphasized that different clients hold different types of rights of Personal Data in different sensitivity levels, for example "medical data," as defined in the Patient Rights Law 5756-1996, personal data, etc.

5.2. With regard to an Israeli service, the Vendor shall not remove Personal Data from the territory of the State of Israel however only after receiving a digital instruction from the client or after obtaining the prior and written approval of the Tender Holder and under conditions that the Tender Holder will see fit.

5.3. With regard to a non-Israeli service, the Vendor shall not remove Personal Data from the territory of a region that is within the EU and the rules of the General Data Protection Regulation (GDPR) shall apply thereto.

5.4. Without derogating from the obligations of the Vendor, the Vendor shall keep protected data that is under its technological control, such as processing data or subscription data in accordance with the provisions of the law and in particular in accordance with the provisions of the Protection of Privacy Law and the regulations enacted thereunder.

6. Criminal prohibition on the exposure of protected data

6.1. The exposure or disclosure of confidential information in accordance with this Agreement, whether by way of an act or omission not in accordance with express and written authorization of the Tender Holder, constitute breach of the duty of confidentiality imposed on the Vendor under this Agreement, and constitute a criminal offense, pursuant to section 118 of the Penal Law 5737-1977.

6.2. In addition, and based on the type of the data that was exposed, the disclosure of protected data, whether by way of an act or omission, not in accordance with the provisions of the Agreement or the provisions of the law, might constitute a criminal offense under Israeli law, based on the type of the data that will be exposed (for example, Personal Data, data under privilege in accordance with the Israeli law, data that can compromise national security etc.).

7. Israeli Service

7.1. The content data shall be fully stored within the territory of the State of Israel, unless otherwise stated in this Agreement.

7.2. Content data that is within State of Israel shall not be removed outside the territory of the State of Israel for any purpose, including for processing, storage, backup or for the purpose of their transfer to a third party without a digital instruction from the client or after obtaining the prior and written approval of the Tender Holder and under conditions that the Tender Holder will lay down.

7.3. If the Vendor removed protected data outside the territory of the State of Israel, the Vendor shall erase the protected data immediately, and to the extent that such action was performed for the purpose of providing a service in accordance with a digital instruction, immediately after the completion of the action, in accordance with the terms set forth in the digital instruction and subject to the provisions set forth in any law.

7.4. In any event, the Vendor shall not keep protected data in a state that does not maintain diplomatic relations with the State of Israel.

7.5. The provisions set forth in this section shall apply to a service operating in an overseas region, *mutatis mutandis*.

8. Governing law and jurisdiction over protected data

8.1. Without derogating from the provisions of section 15.2 of the Agreement:

8.1.1. The State of Israel has full and exclusive sovereign interest and full authorities and rights of ownership in the protected data. As such, the law governing the protected data shall be the laws of the State of Israel and the courts in the State of Israel shall have exclusive jurisdiction over any question or proceeding in connection with the said data, without qualifications or exclusions.

8.1.2. The Israeli law shall govern any direct dispute between the Vendor and the Tender Holder in connection with the protected data, and the courts in the State of Israel shall have exclusive jurisdiction over any question or proceeding in connection with the said data, without qualifications or exclusions.

8.2. The Vendor shall notify immediately regarding any changes or updates in the legal status applicable to the Vendor, that affects the performance of the obligations and the rights in connection with the protected data under this Agreement. For the avoidance of doubt, such a change as said shall not release the Vendor from its obligations in accordance with the provisions set forth in the Agreement.

9. Unlawful transfer of data

9.1. Notwithstanding the provisions of section 8.1.1, if the Vendor received a request or an order by a foreign entity for the purpose of obtaining protected data, its erasure, alteration, or denial of access thereto, and the Vendor is of the opinion that the request or the order as said are legally binding on it, whether or not the data is within the State of Israel, the Vendor shall act in accordance with the following provisions:

9.1.1. The Vendor shall notify regarding the request or the order to the Tender Holder and the relevant client at the earliest opportunity, and shall update them regarding the steps that the Vendor performed until that stage, unless the Vendor is expressly prohibited by law from acting in such manner as said.

9.1.2. To the extent that there is a gag order on the mere data request, the Vendor shall act for the purpose of lifting this order, and for notifying the Tender Holder regarding the mere existence of the request.

9.1.3. The Vendor shall refuse to transfer the data, and shall raise all legal claims that are relevant, including that the data is the property of a sovereign state and that the data is subject to state immunity.

9.1.4. If necessary, the Vendor shall file an appeal on the decision with the relevant competent court or the administrative authority, and until exhausting all possible appellate options, and shall file an application to stay the execution until a final decision on the subject is made.

9.1.5. According to the request made by the Tender Holder, the Vendor shall request to add the State of Israel as a relevant party to the proceeding.

9.1.6. The Vendor shall take measures for the purpose of reducing the scope of exposure of the data solely to the data that is relevant to the request.

9.1.7. The Vendor shall demand that the requirements made in the request or the order shall be observed in accordance with the instructions set forth in mutual legal assistance treaties and shall not act in accordance with the instructions set forth in the request or the order unless this is possible under the law in the place where the protected data is situated.

9.2. In addition to the aforesaid, if the Vendor received a request or an order by a foreign entity for the purpose of obtaining protected data held in the State of Israel, and the Vendor is of the opinion that the said order is legally binding on it, in addition to the provisions set forth in section 9.1, the Vendor shall act as follows:

9.2.1. The Vendor shall act in accordance with the provisions set forth in the Israeli law for the purpose of enforcing the order (for example, in accordance with the provisions of the Foreign Judgments Enforcement Law, 5718-1958, the International Legal Assistance Law 5758-1998 etc.).

9.2.2. In any event, the Vendor shall not enforce an order that was issued by an organ of a foreign country on protected data of the

Government of Israel that is within the State of Israel, if such an action is not permitted under Israeli law.

9.3. Without derogating from the obligations of the Vendor in any other place, the provisions of this section shall apply to the Vendor even if the request is made from a foreign entity and was received by a secondary processor or another subcontractor operating on behalf of the Vendor for the purpose of performing the Services under the Agreement, and that possesses the protected data. In such circumstances as said, the Vendor shall step in and take over the processor or the subcontractor and shall act according to the said obligations.

9.4. To the extent that the Vendor has an indication that such a request or an order is expected to be received in accordance with the provisions of sections 9.1 and 9.2 above, the Vendor shall notify the Tender Holder about the said forthwith, unless there an impediment by law prohibiting the Vendor from acting in such manner.

9.5. Required actions in the event of transfer of protected data

9.5.1. Without derogating from the liability of the Vendor under any law, and without diminishing from its obligations under this Agreement, in any event in which the Vendor transferred protected data to a third party that is not authorized to obtain the data in accordance with the rules set forth in the Tender, for any reason, including as a result of a request or an order issued by a foreign entity, the Vendor shall act as follows:

9.5.1.1. The Vendor shall notify the Tender Holder at the earliest opportunity regarding any protected data that the Vendor provided as said, the scope of the data, the identity of the data recipient, the reasons for the provision of the data, whether the data was encrypted or protected by other security tools, and any other relevant information, unless the Vendor is prohibited by law from performing such actions.

9.5.1.2. The Vendor shall not perform any action that can assist in the decoding or the elimination of any technological barrier from protected data in any manner and form, whether by way of an act or omission. If a request as

said was received from a law enforcement authority or a security authority of a foreign state for decoding or for making accessible protected data, the Vendor shall contact the Tender Holder and request its approval for the purpose of providing such assistance as said, and shall act in accordance with the instructions of the Tender Holder.

9.5.1.3. If the protected data was transferred without notifying the Tender Holder (whether an order prohibiting the mere disclosure of the demand to transfer the data was issued, whether this is a demand of a security authority and whether for any other reason) the Vendor shall pay to the Tender Holder special damages in the amount of ILS 10,000 within a period of 24 hours from the time the data was provided.

9.5.2. The provisions of this section shall not derogate from the liability of the Vendor and its obligation by law and in accordance with the provisions of the Agreement not to disclose protected data without obtaining the prior and written approval of the Tender Holder and shall not derogate from any right to damages, indemnity, or any other remedy that the Tender Holder may seek in accordance with the provisions set forth in the Agreement.

Appendix D – Undertaking of Confidentiality

Entered into and executed in _____ as of this ___ day of _____ 20__

By the authorized signatories on behalf of: _____ (hereinafter: the "Vendor")
Names of signatory(s): _____
ID. No. _____
Address of corporation: _____

Whereas an Agreement was signed for the performance of the Pilot Period between the National Cyber Directorate (hereinafter: the "Directorate") and the Vendor, as stated in the Agreement that was signed between the parties;

And whereas: the Vendor might be exposed to professional secrets and the data that the Directorate is interested to protect;

Therefore, the Vendor undertakes towards the State of Israel as follows:

Definitions

In this Undertaking the following terms shall have the meaning set forth beside them below:

The "Services" – the services that are provided within the framework of the Pilot Period, aforesaid in the Agreement that was signed between the parties.
"Employee" – each of the employees of the Vendor that will provide the Services to the Directorate.
"Information" – any information, know-how, knowledge, document, correspondence, plan, data, model, opinion, conclusion, information security procedures and physical security, and any other thing connected to and/or relating to the performance of the Services, whether written and whether verbal, and/or in any other manner of saving information in an electrical and/or electronic and/or optic and/or magnetic and/or other manner.

"Professional Secrets" – any information that will reach the Vendor or anyone acting on its behalf in connection with the Services, whether received during the performance of the Services or thereafter, including but without limiting the generality of the foregoing: information that the Directorate and/or any other entity and/or anyone acting on its behalf will provide.

Undertaking of confidentiality

The Vendor undertakes to keep in strict confidence the mere performance of the Pilot and the Information and/or the Professional Secrets and use them solely for the purpose of providing the Services subject matter of this Agreement. This shall be done for security reasons, *inter alia*.

For the avoidance of doubt, and without prejudice to the generality of the foregoing, the Vendor undertakes not to publish, transfer, notify, convey, or communicate to any person the Information and/or the Professional Secrets.
I declare that I am aware that failure to perform my obligations constitutes an offense pursuant to Chapter E (Official Secrets) of the Penal Law 5737-1977.

I declare that the Vendor is aware that the disclosure of Personal Data that reaches its possession to an unauthorized entity might also constitute invasion of privacy of a person, an offense liable to legal action pursuant to section 5 of the Protection of Privacy Law 5741-1981.

And in witness whereof I am hereby undersigned:

_____	_____	_____
Date	Name	Stamp of Corporation

Confirmation of attorney

I, the undersigned, _____ Adv., confirm that on _____ Mr./Mrs. _____ who identified himself/herself by ID. No. _____/whom I know in person, appeared before me, in my office in _____ St. in the town/city of _____ and after I warned him/her that he/she is required to declare the truth, and that his/her failure to do so shall subject him/her to statutory penalties, he/she confirmed the truthfulness of this Affidavit and signed it in my presence.

_____	_____	_____
Date	License No.	Signature and Stamp

Chapter E – Agreement

Agreement with the Winning Vendor

Entered into and executed in _____ as of this ___ day of _____ 202_

Between: The Government of Israel in the name of the State of Israel
By the National Cyber Directorate in the Prime Minister's Office
10 HaBarzel St., Tel Aviv - Yafo
(Hereinafter: the "**Directorate**")

The first party;

And between: _____
Address _____
(Hereinafter: the "**Vendor**")

The second party;

Whereas: The Directorate wishes to purchase services for the denial of access to malicious domains and the option to enforce redirection to an approved server (the "**Services**");

And whereas: For the purpose of receiving the Services the Directorate published Tender no. 1-1.2024 - "TAFNIT" (PDNS) - Services for the denial of access to malicious domains and option to enforce redirection to an approved server (the "**Tender**");

And whereas: The Vendor submitted a bid in the Tender and the Vendor agrees to provide the Services in accordance with the terms set forth in the Tender documents and this Agreement including Appendixes thereof;

And whereas: The Tender Committee on behalf of the Directorate selected the bid that was submitted by the Vendor (the "**Bid**") as the winning bid in the Tender for the provision of the Services, subject to the signing of the Vendor on this Agreement and the performance of the other requirements laid down in the Tender;

Now, Therefore, it is Declared, Stipulated and Agreed between the Parties as Follows:

1. **General**

1.1. The following Appendixes are attached to this Agreement:

1.1.1. **Appendix A** – The entire Tender (including all its stages) and the files containing the clarification questions and the answers.

1.1.2. **Appendix B** – The Vendor's Bid Appendix including the price bid.

1.1.3. **Appendix C** – Data processing.

1.1.4. **Appendix D** – Security certificate and confidentiality statement.

1.1.5. **Appendix E** – Digital guarantee printout.

1.1.6. **Appendix F** – Insurance requirements.

1.2. The preamble to this Agreement and Appendixes thereof constitute an integral part hereof.

1.3. The terms used in this Agreement shall have the meaning ascribed thereto in the Tender. The interpretation of the Agreement including Appendixes thereof shall be performed in a manner that is consistent with the express and implied requirements laid down in the Tender and the purpose of the Tender for the performance of the Services to the Directorate in an optimal manner.

1.4. In the event of discrepancy between this Agreement and one of its Appendixes or between the provisions of the Agreement and any other provision relating to the Service (such as licensing agreement, use agreement, End User License Agreement) in a manner that cannot be resolved in accordance with the rules of interpretation set out above, the provisions of the Agreement shall take precedence.

2. **Terms of use of the Services**

2.1. The Directorate shall be entitled to make any use of the Service within the framework of the performance of its roles and its purpose for the State of Israel and its citizens, subject to the provisions of the law applicable to it. In

addition to the provisions set forth in this section, there shall be no limitation of any kind, including rules of "permitted use" in the Vendor's Service.

2.2. Any information of security value that will be produced as a result of the use of the Services and the products of the Vendor within the framework of the Service performed under this Agreement will be shared with other entities and organizations, with or without information from other sources of the Directorate, according to the requirements of the Directorate and its procedures within the framework of the performance of its duties. Notifications of the Directorate that are made public in the information distribution channels of the Directorate may also include raw data from the Service.

2.3. Notwithstanding the aforesaid, a client or anyone acting on its behalf shall not use the Services for the following purposes:

2.3.1. Use for commercial purposes such as resale.

2.3.2. Infringement of the intellectual property rights of the Vendor including the performance of reverse engineering.

2.4. There shall be no limitation on behalf of the Vendor on the types of the data that the clients may migrate to the Service including data that is highly sensitive.

2.5. There shall be no limitation preventing from the clients to transfer content data, including the logic that was defined by the client to another entity, including a cloud provider or another service.

3. **Term of engagement**

3.1. The term of engagement under this Agreement is for a period of 3 years as of the date the Tender Holder delivered notice regarding the commencement of the engagement (the "**Term of Engagement**").

3.2. The Directorate shall have the option to expand and/or extend the Term of Engagement by additional periods that shall not exceed 7 additional years (a total of up to 10 years as of the signing date of this Agreement), in accordance with the provisions set forth in this Agreement and subject to the provisions of the Mandatory Tender Law.

3.3. The option right shall be exercised as long as the Office wishes to continue and receive the Services. The Agreement shall be extended in accordance with the terms set forth under the original agreement, or under conditions that are favorable to the Directorate that will be agreed in writing between the parties.

3.4. **It is clarified that the engagement by virtue of the Tender is conditional on the existence of a budget**.

3.5. Prior to the expiration of the Term of Engagement, the Directorate shall be entitled to perform a gradual process for the replacement of the Vendor with a new vendor (the "**Transition Period**"), and the Directorate shall notify the Vendor regarding the commencement date of the said Transition Period. The Directorate shall decide on the length of the said Transition Period, however in any event the said period shall not exceed three months. During the said period of time, the Vendor shall be obligated to continue and provide the Services that the Vendor provides in accordance with this Agreement, in a scope prescribed by the Directorate and according to the prices as stated in **Appendix B**, until the completion of the transfer of the Services to the new vendor, as stated in section 17 of this Agreement. The Vendor shall fully cooperate with the Directorate and with the new vendor and shall assist it in anything required for the purpose of performing the transition.

4. **Ordering services**

4.1. The Directorate shall have the option to increase or decrease the entire components that are purchased within the framework of the engagement, at any time during the Term of Engagement, for the prices as stated in **Appendix B**.

4.2. Procurement of supplementary services and products:

4.2.1. The Directorate shall have the option to purchase supplementary services and products to the Services that are provided in accordance with the Tender and this Agreement, whether directly by the Vendor and whether by an integration with third-party vendors, for a discount percentage that will be no less than 25% of the price as stated in the price list of the Vendor that was attached to Appendix B or the updated price list at the time (whichever is cheaper).

4.2.2. The Vendor shall be entitled to submit an updated price list once a year, for supplementary services and products, on the condition that after the update the price of each product or service shall not exceed by more than 5% compared to the previous price list that was submitted, to the extent that it was submitted.

4.2.3. The updated price list shall be delivered to the Directorate one month prior to the end of each year of engagement and shall enter into force with respect to this Agreement starting from the commencement of the subsequent year of engagement, to the extent realized.

5. Undertakings and declarations of the Vendor

5.1. The Vendor declares and undertakes as follows –

5.1.1. It possesses the experience, competence, know-how, tools, equipment, inventory, and the manpower that are required for the purpose of providing the requested Services, in accordance with the terms set forth in the Agreement and the Tender.

5.1.2. It complies with the entire relevant provisions of the law for the purpose of performing the Services in accordance with this Agreement and in any event of a change in the provisions of the law, the Vendor shall incur the costs in connection with the said changes.

5.1.3. The requested Services that the Vendor shall supply shall comply with the requirements laid down in the Tender.

5.1.4. It shall cooperate with the Directorate in anything related to the performance of its obligations in accordance with this Agreement.

5.1.5. It shall take measures for the proper storage and security of the entire equipment in its possession and that is related to the performance of its obligations under this Agreement against theft, fire, loss, dampness or any other harm.

5.1.6. It shall be held liable for any damage caused to the entire equipment in its possession and that is related to the performance of its undertakings under this Agreement until the date of completion of the performance of the Service.

5.1.7. It shall fully cooperate with the different security and safety units in the Directorate, and shall observe their instructions.

5.1.8. During the entire Term of Engagement, it shall provide to the Directorate the official, full and latest version of the Services. In the event that during the Term of Engagement the Vendor releases version updates to the Services that are provided, it shall provide to the Directorate the Services in their official, full and latest version (General Availability).

5.1.9. In addition, the Vendor shall offer to the Directorate the option to use new BETA versions of the Service in the manner decided by the Directorate.

5.1.10. There is no impediment under any law prohibiting its engagement in this Agreement and the performance of the Agreement by the Vendor shall not give rise to any conflict of interests, whether directly or indirectly, between the Vendor and the Directorate.

5.1.11. In any event that there is any concern regarding a conflict of interests between the Vendor and the Directorate the Vendor shall notify promptly the Directorate regarding such a concern as said, and shall take measures to eliminate such a conflict of interests as said.

5.1.12. The actions of the Vendor within the framework of this Agreement, including its products, the Services and the software tools that the Vendor will use within the framework of the Agreement are performed and implemented in accordance with the provisions of the law in Israel and the software, the products, the Service or any other action of the Vendor that are part of the performance of the Services for the Directorate in accordance with this Agreement do not constitute any violation of the law including, but not limited to,

in connection with intellectual property laws, computer laws and protection of privacy laws.

5.1.13. The Vendor undertakes that the Service shall be provided by the cloud providers that won the NIMBUS Tender - Central Tender 01-2020 for the provision of cloud services on a public platform for the government ministries and auxiliary units (hereinafter: the "NIMBUS Tender") and undertakes that after setting up a data center in Israel by the cloud provider with which the Vendor engaged – it shall ensure that the entire data relating to the Services that are provided within the framework of this Tender shall be transferred to the Israeli data center, according to the requirements laid down in the Tender and in accordance with the provisions of Appendix C of this Agreement.

6. Relationship between the parties

The parties hereby declare and agree as follows:

6.1. The relationship between the parties under this Agreement give rise to a relationship between a Tender Holder and a service provider only, and shall not give rise to employer-employee relationship.

6.2. The Directorate shall not pay any payment to the National Insurance Institute and other social-benefit payments in connection with the persons who are employed by the Vendor.

6.3. The Vendor shall be held solely liable for any payment, indemnity for any damage or damages or any other payment that is due from the Vendor in accordance with the law to the persons that the Vendor employs, or to any other person, for actions that the Vendor performed.

7. Consideration

7.1. In return for the performance of the entire undertakings of the Vendor in accordance with the Tender and this Agreement, the Directorate shall pay to the Vendor according to the prices as stated in the price bid of the Vendor, in Appendix B, and based on the number of organizations that are monitored and the number of users (hereinafter: the "**Licenses**") that the Directorate will purchase (hereinafter: the "**Consideration**") to the extent that the

number of Licenses increases or decreases in a manner that will transfer the purchased amount from one category to another, the balance of the Consideration that will be paid to the Vendor as of the date of the change shall be made after performance of setoff of the Consideration that was already paid.

7.2. The Consideration shall be paid in advance, once a quarter in the beginning of the quarter, subject to receiving a demand for payment by invoice from the Vendor, that will include information regarding the number of the organizations that are monitored and the users in respect of which the demand for payment was delivered. It is clarified that the demand for payment will include only licenses that were actually activated. One month prior to the end of each year of engagement, the parties shall conduct an inspection of the number of the monitored organizations and the users that the Directorate added or removed during the year, and additional payments or setoffs shall be made, as may be required. Payment for a user and/or a monitored organization that was active for only part of the year shall be made according to the calculation of the relative part out of the user's cost per year.

7.3. Notwithstanding the provisions of section 7.2 above, the Consideration for the last quarter of the engagement shall be paid at the end and not in the beginning of the quarter. One month prior to the end of the last quarter of the engagement, the Vendor shall be obligated to submit an annual report of the number of the monitored organizations and the users during the year for the purpose of making a final calculation of the final bill for payment. This payment shall include additional payments or setoffs as may be required, based on the actual number of monitored organizations and users, and payment in respect of a user or a monitored organization that was active for only part of the year shall be paid based on a calculation of the relative part out of the user's cost per year. The addition of Services or monitored users/organizations shall not be permitted in the last month of the engagement.

7.4. Notwithstanding the said, the Directorate shall be entitled to decide to pay in advance the Consideration for the first year or the first two years or for three years in advance.

7.5. Statutory VAT charged with respect to the said prices shall be added to the Consideration and shall be paid according to each invoice/payment that the Directorate will pay.

7.6. To the extent that the Vendor is an Israeli company, payment shall be made in shekels. To the extent that the Vendor is a foreign company, payment shall be made in a foreign currency out of the following foreign currencies: U.S. dollar, euro, pound sterling, in the manner agreed between the Directorate and the Vendor. In the event of payment in a foreign currency, payment shall be made based on a calculation of the price in shekels as stated in Appendix B, according to the representative exchange rate that was published by the Bank of Israel and known on the payment date. All payments shall be made subject to the instructions of the Accountant General in the Ministry of Finance regarding the manner of execution of payments as published from time to time.

7.7. The Vendor shall be required, subject to the decision of the Directorate and at its discretion, to submit reports and bills that are required for the purpose of making payment. To the extent that the Vendor is an Israeli corporation, the Vendor shall be obligated to submit the required reports and bills in the government suppliers portal, according to the terms of use in the suppliers portal, and shall incur all costs in connection with the connection to the government suppliers portal, to the extent that there are any, in accordance with the instructions set forth in TAKAM Directive no. 7.12.5, "Suppliers Portal." Alternatively, if the Bidder uses the suppliers portal, the Bidder shall provide a confirmation for the purpose of this matter.

8. **Management of users**

8.1. The following conditions shall apply, *inter alia*, to the opening and management of users:

8.1.1. The Directorate shall have the option to allow the use of the Services that are provided within the framework of this Agreement also to the users on behalf of other government ministries, Critical Cyber Infrastructure entities or other entities that will be defined by the Directorate as relevant (the managed organizations), including the operation of the national CERT (that includes, *inter*

alia, sectorial SOC centers that are operated by the government ministries within the framework of the national CENTER activity).

8.1.2. Users from other government offices, as stated in section 8.1.1, shall be registered under the domain name of the Directorate or any other domain name, in the manner selected by the Directorate.

8.1.3. The Directorate shall have the option to assign users that will be defined as "team users" and designated for work in shifts; these users shall not be assigned to a specific person, but a specific role (for example – on-call SOC analyst). At any given moment there shall be not more than one person making use of this type of user.

8.1.4. It is clarified that in any event the engagement under this Agreement is made directly with the Directorate and the Directorate shall be responsible towards the Vendor for the payment of the consideration.

9. **Protection of confidentiality, no publication, and data security**

9.1. Information for the purpose of this section shall mean any information that was inputted by the users in the Service (including queries and searches and intelligence information inputted in the Service), information containing details of the Vendor's users, or the details regarding the use that the Directorate makes with the Service, and any information related to the Tender specification

9.2. The Vendor hereby declares that it is aware that the information to which the Vendor will be exposed during the performance of the Services in accordance with this Agreement has special sensitivity, and the Vendor undertakes that it and anyone acting on its behalf shall keep the information in strict confidence and shall not make any use of the said information, except for the performance of the Services in accordance with the Tender and this Agreement. For the avoidance of doubt, and without prejudice to the generality of the foregoing, the Vendor undertakes that it and anyone acting on its behalf shall not publish, transfer, notify, communicate, or disclose to any person the information, except for information that is in the public domain, or information whose provision is mandatory by law. Failure to perform this undertaking might constitute an offense pursuant to Chapter

G (National Security, Foreign Relations, and Official Secrets) of the Penal Law 5737-1977.

9.3. In addition, and based on the type of the data that was exposed, the disclosure of protected data, whether by way of an act or omission, not in accordance with the provisions set forth in the Israeli law, based on the type of the data that will be exposed (for example: personal data, data under privilege under Israeli law, data that can compromise national security etc.).

9.4. The Vendor undertakes to sign each of the employees that the Vendor will employ for the performance of the Services for the Directorate by virtue of this Tender, including its subcontractors and anyone exposed to the data relating to the engagement, on the Confidentiality Statement in the form attached as **Appendix E** of this Agreement. In addition, to the extent that the Vendor hires new employees for the purpose of providing the Services as said, the Vendor shall sign them promptly on such an undertaking as said.

9.5. The Vendor undertakes not to advertise any information relating to the Directorate or the existence of the engagement or the performance of the engagement with the Directorate without obtaining the prior and written approval of the Directorate.

9.6. The obligations of the Vendor with relation to the data shall apply as long as the Vendor holds the data, even after expiration of the Term of Engagement.

10. **Supervision over the Vendor's work**

10.1.1. The Directorate shall be entitled to conduct, at its discretion, or demand from the Vendor, to conduct random tests or receive information for the purpose of examining the Services that will be provided in accordance with the provisions set forth in the Tender and this Agreement.

10.1.2. The Vendor or the subcontractor on its behalf (except for third-party data storage facilities) shall allow the Directorate or whoever is appointed on its behalf to supervise the performance of the requested Services, including their nature and quality, and enter to any place for the purpose of this matter, for the purpose of

inspecting and supervising the manner of performance of its undertakings. In the event it is necessary to enter the Vendor's premises for the purpose of this matter, the visit shall be scheduled in advance, and the Vendor undertakes to answer the request for a visit in 7 business days.

10.1.3. The Directorate shall be entitled to appoint a supervisor on its behalf for the purpose of examining and supervising the Vendor's work. The Vendor undertakes to cooperate with the representatives on behalf of the Directorate and with the supervisors on its behalf.

10.1.4. The Vendor shall provide to the representative on behalf of the Directorate and the supervisors any information or report that will be demanded by them and that are relevant for the purpose of providing the Services to the Directorate, based on the opinion of the Directorate, on the date and in the manner decided by them, shall allow to the representatives on behalf of the Directorate and the supervisors to visit its offices and in any other place where the Vendor performed its undertakings in accordance with this Agreement (except for third-party data storage facilities), inspect any document that is relevant to the supply of the Services according to the opinion of the Directorate, and inspect everything performed therein in connection with the Services and the performance of the undertakings of the Vendor in accordance with this Agreement, and provided that each visit as said is scheduled in advance with the Vendor.

10.1.5. For the avoidance of doubt, it is clarified and agreed that the representatives on behalf of the Directorate and the supervisors shall not be entitled to and are not authorized to impose on the Directorate any financial obligation that will change the amount of the Consideration in accordance with this Agreement, and that will impose additional financial obligations in connection with adjustments, and the amounts charged from the Directorate for the purpose of this matter shall be executed solely in a written document, signed by the authorized signatories on behalf of the Directorate.

11. **Availability of the Service**

11.1. The Vendor undertakes that the Service shall be available 24 hours a day, 7 days a week, except for short and scheduled downtime periods for maintenance and upgrade purposes in respect of which the Directorate shall receive a one month prior and written notice. The Vendor further undertakes that the total availability of the Service on annual average shall be no less than 99.9999% availability (hereinafter: the "**Total Annual Availability**") and that the availability of the management interfaces (hereinafter: the "**Total Management Interfaces Availability**") on annual average shall be no less than 95%.

11.2. If the availability of the Service is less than the Total Annual Availability or the Total Management Interfaces Availability, the Directorate shall be entitled to extend the Service for no additional payment for a period of one week for each day in which the Service is not available as required.

12. **Cyber incident**

12.1. The Vendor undertakes to act for the purpose of protecting the data of the National Cyber Directorate and the integrity, confidentiality and availability of its data.

12.2. In any event of a cyber-attack or a suspected cyber-attack on the Vendor's systems that are used or that the related to the Services that the Vendor provides to the Directorate, and that might affect the data security of the Directorate, as defined in section 9 of the Agreement, the Vendor shall report to the Directorate promptly and no later than 12 hours as of the time of becoming aware of the attack or the suspected attack, together with the full relevant information that the Vendor knows about the attack, and that might affect the data security of the Directorate, as defined in section 9 of the Agreement, the steps that are taken by the Vendor for the purpose of handling the attack, and the information that was exposed and/or that might be exposed as a result of the attack. The Vendor undertakes to act for the purpose of protecting the system data.

12.3. The Vendor shall report and shall update the Directorate during the response to the attack according to the demands made by the Directorate, and shall cooperate with the requirements made by the Directorate in anything related to the information that was exposed and/or that might be exposed as a result of the attack.

13. **Liability for damages**

13.1.1. The Vendor shall be held liable for any harm, damage or loss of any kind caused to the client, its employees and anyone acting on its behalf and to any entity, person or any other third party, in consequence of an act or omission of the Vendor, its employees, agents, subcontractors or anyone acting in its name and in its place as part of the performance of this Agreement, up to the liability limit set out in section 13.1.5.

13.1.2. The client, anyone acting on its behalf or employed by the client shall not be held liable and shall not incur any payment, expense, harm, loss, or damage in respect of any harm, damage or loss of any kind caused to the Vendor, anyone acting on its behalf or anyone employed by the Vendor. The aforesaid shall not apply to damage that was caused maliciously or as a result of gross negligence and for which the client is held liable by law.

13.1.3. The termination of this Agreement shall not derogate from the liability of the Vendor for damages whose cause of action arises out of this Agreement or from the performance of the Services under this Agreement or in connection therewith.

13.1.4. The Vendor undertakes to pay and indemnify the client fully, to the extent that the organization is obligated to make payment in a peremptory judgment given by a competent court and whose execution was not suspended, to pay any amount in respect of any financial obligation that the Vendor owes in accordance with this Agreement, whether stemming from a claim of an employee of the Vendor or anyone acting on behalf of the Vendor (including subcontractors) or an employee of the client or a third party, or of an insurer or from any other source, up to the liability limit set out in section 13.1.5.

13.1.5. Unless otherwise stated expressly in this Agreement, the liability limit of the Vendor for the payment of damages or indemnity to the client for any damage event shall not exceed the amount of the damage that was caused or the indemnity that is required and up to two times of the scope of actual consumption of the Services from

the Vendor by the Office in the 12 months that preceded the damage event, whichever is lower, and with the addition of the entire expenses of the client, including legal expenses and attorney fees that the Vendor shall incur in connection with a suit brought in connection therewith, and with the addition of linkage differentials and statutory interest. The limitation of liability as said shall not apply to the following: damage caused deliberately to a third party by an act or omission of the Vendor, its employees or anyone acting on its behalf; damage covered under the insurances that the Vendor undertook to take out in accordance with this Agreement; damage to tangible property or damage that constitutes personal injury, death, sickness, physical, mental or intellectual impairment; damage caused as a result of breach of the duty of confidentiality.

13.1.6. The client shall notify the Vendor regarding any claim or demand made under this section at the earliest opportunity after its receipt, and shall afford to the Vendor an opportunity to defend against it. In such circumstances as said, the client shall not agree to the claims that were made or held against the Vendor, and for which the Vendor is held liable in accordance with this Agreement, without obtaining the prior and written approval of the Vendor, and shall notify to the Vendor in advance regarding its intention to settle with the plaintiff.

14. Performance guarantee

14.1. As a security for the performance of the undertakings of the Vendor in accordance with the Agreement, the Vendor shall provide to the Directorate, as a condition for the signing of the Agreement, an autonomous, unconditional digital guarantee, in an amount of 5% of the amount of the Consideration for the annual Term of Engagement, and all as stated in TAKAM Directive 7.3.3 and according to the guarantee form attached as **Appendix E** of the Agreement.

14.2. The guarantee shall be in effect for a period of 90 days after the expiration of the Term of Engagement. In the event that the Directorate extends the option for the extension of the Term of Engagement, the Vendor shall extend the effect of this guarantee respectively until 90 days after the expiration of each period. The guarantee shall be used for the purpose of ensuring the

timely performance of the entire undertakings of the Vendor in accordance with the Tender and this Agreement.

14.3. The Directorate shall be entitled to extend the effect of the guarantee by an additional period of 90 days after the expiration of the Transition Period, in the event that this is necessary for the purpose of ensuring the completion of the performance of the Services or the warranty.

14.4. If the guarantee was not forfeited, the guarantee shall be returned to the Vendor after the expiration of the Term of Engagement and after the Directorate confirms that the products and the Services were provided to its full satisfaction.

14.5. **Forfeiture of guarantee**

14.5.1. The Bid Guarantee any be forfeited by the Directorate in consequence of breach of the Tender or the Agreement by the Vendor or following misconduct or bad faith conduct, or for the purpose of making any other payment due to the Directorate from the Vendor. In addition, the Directorate shall be entitled to forfeit the Guarantee for the purpose of collecting the payment of liquidated damages or for the purpose of recovering other damages due to the Directorate as a result of the Vendor's conduct.

14.5.2. The Vendor shall receive a 5 days' written notice before the Directorate exercises its authorities under this section.

14.5.3. It is hereby clarified that the forfeiture of the Guarantee shall not be deemed as payment of the full damages under this Agreement, and the Directorate shall be entitled to recover from the Vendor the difference between the amount that was paid in consequence of the forfeiture of the Guarantee and the amount of the damage actually sustained by the Directorate.

14.5.4. In any event in which the Guarantee was forfeited, the Vendor shall be obligated to return the Guarantee to its original amount in 30 days as of the forfeiture day of the Guarantee.

15. **Insurance**

15.1. The Vendor undertakes to take out and maintain the insurances as stated hereunder in favor of the Vendor and in favor of the State of Israel – Prime Minister's Office, the National Cyber Directorate, when the said insurances include all coverages and conditions as required hereunder and when the liability limits shall not fall below the liability limit set out hereunder:

15.1.1. <u>Employers' liability insurance (or an equivalent insurance, such as workers compensation)</u>

(1) The Vendor shall take out employers' liability insurance for its statutory liability in accordance with the Tort Ordinance [New Version] and/or the Liability for Defective Products Law, 5740-1980 towards its workers in the entire territory of the State of Israel and in the territories controlled by the IDF.

(2) The liability limit shall be no less than ILS 20,000,000 (or USD 5,000,000) per worker, per event and for the period of insurance.

(3) The insurance shall be extended to provide coverage for the liability of the insured towards contractors, subcontractors, and their workers if the insured is considered as their employer.

(4) The insurance will be extended to indemnify the State of Israel – Prime Minister's Office, the National Cyber Directorate, in the event it is ruled, regarding the occurrence of any occupational accident or an occupational disease, that any of them is held liable as an employer towards any of workers of the Vendor, contractors, subcontractors and workers at their service.

15.1.2. Third-party liability insurance (can be arranged under the CGL insurance)

(1) The Vendor shall take out insurance for its statutory liability in accordance with the laws of the State of Israel in third-party liability insurance for the purpose of covering personal injury and damage to property (including indirect loss) in the entire territory of the State of Israel and the territories controlled by the IDF.

(2) The liability limit shall be no less than ILS 1,000,000 (or USD 250,000) per event and for the period of insurance.

(3) The policy will include a CROSS LIABILITY clause.

(4) The insurance will be extended to cover the liability of the insured towards a third party in respect of the actions of contractors, subcontractors, and their workers.

(5) The insurance will be extended to indemnify the State of Israel – Prime Minister's Office, National Cyber Directorate, to the extent that they are considered as liable for the acts and/or omissions of the Vendor and anyone acting on its behalf.

15.1.3. Professional liability insurance

(1) The Vendor shall take out professional liability or professional liability insurance combined with product liability insurance for its activities in the hi-tech/computers sector.

(2) The policy shall provide coverage for the statutory liability of the Vendor in respect of damage as a result of breach of a professional duty of the Vendor, its workers and anyone acting on its behalf and that occurred as a result of an act, negligence, including an omission, error or failure, misrepresentation, negligent statement made in good faith, in connection with the provision of services preventing

access to malicious domains and the option to enforce redirection to an approved server for the National Cyber Directorate, and that also include the examination of suspicious domains and making a decision regarding the type of response in connection with translation requests relating to them, operation of the management interface and a local management interface for the purpose of managing the service, migrating the data by an interface (API) to other systems, in accordance with the Tender and the Agreement with the State of Israel – Prime Minister's Office, National Cyber Directorate.

(3) The liability limits shall not fall below ILS 10,000,000 (or USD 2,500,000) per event and for the period of insurance.

(4) Coverage under the policy shall be extended to include the following extensions:

- Loss of documents, including loss of use and/or delay in consequence of the occurrence of the insured event.
- Employee fraud and dishonesty.
- Cross-liability, however the insurance shall not provide coverage for claims of the service provider towards the State of Israel – Prime Minister's Office, National Cyber Directorate.
- A minimum discovery period of 6 months.

(5) The insurance will be extended to indemnify the State of Israel – Prime Minister's Office, National Cyber Directorate, to the extent that they are considered as liable for the acts and/or the omissions of the Vendor and anyone acting on its behalf.

15.1.4. General

The following conditions shall be incorporated in all insurance policies required from the Vendor:

(1) The following shall be added to the name of the insured, as additional insureds: State of Israel – Prime Minister's Office, National Cyber Directorate, subject to the indemnity extensions as stated above.

(2) In any event of an adverse change or cancellation of the insurance by one of the parties, the said actions shall be void unless a notice was delivered in a letter to the financial controller in the Prime Minister's Office no less than 60 days in advance.

(3) The insurer waives any right of subrogation, claim, participation, or recourse towards the State of Israel – Prime Minister's Office, National Cyber Directorate, and their workers, provided that the said regarding waiver of the right of subrogation shall not apply in favor of a person who causes damage with malicious intent.

(4) The Vendor shall be held solely liable towards the insurer for the payment of the insurance premiums for all policies and for the performance of all obligations that are imposed on the insured in accordance with the terms set forth in the policies.

(5) The deductibles set out in each policy shall solely apply to the Vendor.

(6) Any section in the insurance policies that forfeits or diminishes in any manner the liability of the insurer when there is another insurance shall not be applied to the State of Israel, and the insurance shall be deemed as primary insurance that grants the entire rights under the insurance.

(7) The intention and/or gross negligence exclusion, to the extent that there is any, will be canceled.

(8) The jurisdiction and territorial borders sections in the policies will also include the State of Israel.

15.2. During the entire term of engagement with the State of Israel – National Cyber Directorate the Vendor undertakes, as long as its liability is in effect, to keep the insurance policies in effect. The Vendor undertakes that the insurance policies will be extended each period of insurance, as long as the agreement with the State of Israel – National Cyber Directorate is in effect.

15.3. The Vendor shall provide to the Prime Minister's Office – National Cyber Directorate a certificate issued with the signature of the insurer confirming the existence of the insurances until the signing date of the Agreement. The Vendor undertakes to present the certificate regarding the extension of the insurances signed by its insurer to the Prime Minister's Office, the National Cyber Directorate, in seven days prior to the expiration of the period of insurance at the latest.

It is hereby clarified that the certificates of insurance that will be presented are not intended to diminish and/or derogate from the undertakings of the Vendor to take out the insurances according to the insurance sections as stated above and, for the avoidance of doubt, the binding insurance requirements are made in accordance with the requirements laid down above. The Vendor is required to learn and comply with the said requirements and, if necessary, receive assistance from insurance consultants on its behalf, for the purpose of complying and implementing the said requirements in its insurances, as required.

15.4. The State of Israel – Prime Minister's Office, National Cyber Directorate, reserves the right to obtain from the Vendor at any time the policies, in whole or in part, in the event of discovery of circumstances that might result in a claim in the policies and/or for the purpose of examining the compliance of the Vendor with these actions and/or for any other reason, and the Vendor shall deliver the copies of the policies, in whole or in part as said, immediately after receiving the said demand. The Vendor undertakes to make any change or amendment that will be required for the purpose of making the policies in conformance to its undertakings in accordance with the insurance provisions set forth above. It is agreed that the Vendor shall be entitled to remove from the insurance policies as said confidential business and/or commercial information that is irrelevant to this engagement.

The Vendor declares and undertakes that the right of the State of Israel – Prime Minister's Office, National Cyber Directorate to conduct the inspection and demand the changes as stated above shall not impose on the State of Israel – National Cyber Directorate or anyone acting on its behalf any obligation and any liability in connection with the insurance policies/certificates of insurance as said, including their essence, nature and validity, or lack thereof, and shall not derogate from any obligation that is imposed on the Vendor in accordance with this Agreement, whether or not such modifications were required, and whether or not the said insurances were inspected.

15.5. **For the avoidance of doubt, it is hereby agreed that the insurances required under this insurance section, the liability limits and the terms of coverage are a minimum requirement imposed on the Vendor, and do not constitute confirmation by the State or anyone acting on its behalf regarding the scope and the extent of the insured risk and the Vendor is required to examine its exposure to the risks and take out the insurances that are required, including the scope of coverages, the period of insurance and the liability limits accordingly.**

15.6. Anything stated in the insurance sections shall not exempt the Vendor from any obligation imposed on the Vendor in accordance with the law and in accordance with the Agreement, and the aforesaid shall not be construed as waiver by the State of Israel – Prime Minister's Office, National Cyber Directorate of any right or relief they may seek under any law and in accordance with this Agreement.

15.7. Failure to satisfy the conditions set out in these insurance sections constitutes a fundamental breach of this Agreement.

16. **Termination of the engagement**

16.1. Without derogating from any other provision in the Agreement, it is hereby agreed that the Directorate shall be entitled to notify the Vendor, by delivery of a 30 days' prior and written notice, regarding the termination of operations under this Agreement for any reason, and the Directorate shall not be obligated to give reasons for its decision.

16.2. It is agreed and declared that the Vendor shall have no financial claim or demand or any other demand towards the Directorate in connection with the termination of its operations as said, except for the payment for the Services that the Vendor already provided.

16.3. To the extent that the Vendor received advance payment for the Services or a part thereof, the Vendor undertakes to return the said payments for the period in which the Services are not provided as a result of the termination of the engagement.

17. Transition period

17.1. It is agreed that during the transition period the Vendor shall be required to act at the earliest opportunity and without delay, as follows:

17.1.1. The Vendor shall appoint the project manager on its behalf as the manager of the separation plan.

17.1.2. The Vendor undertakes to provide to the Office in an organized manner the entire data, information and know-how that the Vendor accumulated during the performance of the activity, and the entire deliverables that were created during the performance of the Services, when they are updated, readable and in formats that were defined and approved by the Directorate in advance.

17.1.3. Without derogating from the foregoing, the Vendor shall provide to the Directorate all deliverables that the Vendor created as part of the performance of the Services.

17.1.4. The transfer of the data and the information shall be performed by the Vendor in a manner that will prevent damage or malfunctions or service discontinuity.

17.1.5. The Vendor shall prepare a work plan for separation and on-the-job training according to its bid in the Tender, and shall submit the said plan for the approval of the Directorate in two weeks as of the date of receiving the notice regarding the commencement of the transition period.

17.1.6. The Vendor shall fully cooperate with the Directorate and with the entity designated as the Vendor's substitute (to the extent that there is any) and shall act in accordance with the plans as stated above, for the purpose of facilitating the organization, replacement, and normal continuation of the activity after termination of the engagement with the Vendor.

17.1.7. The Vendor shall permit to the representatives on behalf of the Directorate to meet with any officer related to the performance of the Services (and, to the extent possible, also a former officer related to the performance of the Services) for the purpose of performing on-the-job training and/or mapping and documenting the knowledge and information held by the Vendor.

17.1.8. The Vendor shall continue to handle all tasks under its responsibility, until the termination of the engagement and the completion of the transfer of the information and the knowledge as said.

17.1.9. After completion of the separation, the Vendor undertakes to erase and destroy any copy of the information in its possession, in coordination with the Directorate, unless the Directorate ordered otherwise and in writing. It is clarified that the Vendor shall not be required to erase information that was in its possession by law prior to the commencement of the Services contemplated in this Tender.

18. Breach of the Agreement

18.1. The following shall be deemed as a fundamental breach of this Agreement (hereinafter: "**Fundamental Breach**"):

18.1.1. Substantial deviations from the terms of the Services requested in the Tender;

18.1.2. Breach of the following sections in the Agreement: 2, 4, 5, 9, 11, 14, 15 and 17.

18.1.3. Without prejudice to the generality of the foregoing, each of the following actions shall be deemed as a Fundamental Breach of the Agreement:

18.1.3.1. Provision of Services that fail to comply with the requirements laid down in the Tender and the Agreement.

18.1.3.2. Working with a subcontractor in violation of the provisions set forth in the Tender and in the Agreement.

18.1.3.3. Failure to provide Services to the Directorate in accordance with the requirements laid down in the Tender and the Agreement.

18.1.3.4. If an interim liquidator, a temporary liquidator, or a permanent liquidator is appointed for the Vendor; and it is clarified that upon the occurrence of the event as stated above the Vendor shall be obligated to notify the Directorate at the earliest opportunity regarding such an appointment as said.

18.1.3.5. If a temporary or permanent receiver is appointed for the business and/or the property of the Vendor; and it is clarified that the Vendor shall be obligated to notify the Directorate at the earliest opportunity regarding such an appointment as said.

18.1.3.6. If a stay of proceedings order is issued against the Vendor; it is clarified that the Vendor shall be obligated to notify the Directorate at the earliest opportunity regarding the issuance of such an order as said.

18.1.3.7. If the Vendor discontinued conducting its business for a consecutive period exceeding 30 days; it is clarified that the Vendor shall be obligated to notify the Directorate at the earliest opportunity regarding such discontinuation as said.

18.2. If the Vendor committed a Fundamental Breach, the Directorate shall be entitled, at its discretion, to discontinue forthwith the engagement with the Vendor or any part thereof, without additional notice, and terminate the Agreement, without derogating from the right of the Directorate to a relief or to damages, as stated in the Tender, the Agreement or under any law.

19. **Remedies in consequence of breach of the Agreement**

19.1. **Termination of the engagement in consequence of a breach**

19.1.1. Without derogating from the foregoing, the Directorate shall be entitled to terminate the engagement in consequence of a breach committed by the Vendor upon the occurrence of the following events:

19.1.1.1. In any event the Vendor failed to fulfill its undertakings in accordance with the Tender and the Agreement, for any reason, or failed to cure the breach in 15 workdays as of the date of receiving written notice from the Directorate.

19.1.1.2. If the Vendor learned that it was possible that it would not be able to fulfill its undertakings, in whole or in part, for any reason, or that the Vendor will not be able to meet the dates and the conditions of the service, the Vendor shall notify forthwith verbally and by email to the Directorate about the said events. If the Vendor delivered such notice as said, the Directorate shall be entitled, at its discretion, to allow the Vendor to prepare a plan to rectify the defects and discuss such a plan, or terminate the engagement with the Vendor or any part thereof.

19.1.2. In any event of termination of the Agreement in consequence of a breach committed by the Vendor, the Vendor undertakes to continue with the performance of the requested services to the Directorate, in return for payment for these services, in accordance with the terms set forth in the Tender, unless the Directorate decides otherwise and notifies the Vendor in writing about its decision.

19.1.3. The provisions set forth in this section shall not derogate from the right of the Directorate to obtain any other relief under this Agreement or under any law in respect of the breach.

19.2. **Setoff and withholding**

19.2.1. Without derogating from the rights of the Directorate under this Agreement or under any law, the Directorate shall have a right of setoff from amounts that the Directorate owes the Vendor in accordance with the Agreement for any debt that the Vendor owes to the Directorate, whether or not specific. In addition, the Directorate shall be entitled to withhold any amount that the Directorate owes to the Vendor, until the Vendor pays any payment that the Vendor owes to the Directorate.

19.2.2. The Vendor shall have no right of setoff or withholding towards the Directorate in respect of any amount the Directorate owes to the Vendor, based on its claim.

20. **Cumulative remedies**

20.1. The remedies, including the right of setoff and forfeiture, liquidated damages, and all actions that the Directorate is entitled to perform in this Agreement in response to the breach of the Agreement by the Vendor, are cumulative, and none of the provisions set forth in this Agreement shall deny from the Directorate its right to seek any relief or remedy in accordance with this Agreement or under any law.

20.2. If the Directorate waived its rights in consequence of breach of any of the provisions set forth in this Agreement by the Vendor, the waiver shall not be deemed as waiver of another breach of the said provision or of another provision.

21. **Assignment of rights or obligations under the Agreement**

21.1. The Vendor is strictly prohibited from assigning or endorsing any right or obligation under this Agreement or the performance of the actions under this

Agreement or any part thereof to another, without obtaining the prior and written approval of the Directorate, at its sole discretion.

21.2. If the Directorate agreed that the Vendor will assign or endorse its rights or obligations under this Agreement, such approval by the Directorate shall not release the Vendor from its liability towards the Directorate in connection with the provisions set forth in this Agreement.

21.3. It is hereby declared and agreed that the Directorate shall have the right to assign or endorse any right or obligation under this Agreement without obtaining any approval from the Vendor or from any other third party.

22. **Modification**

Any modification of this Agreement shall be null and void unless executed in advance in writing and signed by the parties.

23. **Addresses of the parties and notices**

23.1. Address of the Directorate: National Cyber Directorate, 10 HaBarzel St., Tel Aviv – Yafo.

Address of Vendor: _____.

23.2. Any notice delivered in accordance with this Agreement shall be delivered in registered mail, unless the parties agreed otherwise and in writing; a notice in registered mail as said shall be deemed to have reached its recipient 3 days as of the date of its delivery from the post office.

23.3. A receipt bearing the stamp of the Israel Postal Company shall be deemed as proof of the delivery date.

24. **Exclusive jurisdiction**

The parties submit to the sole jurisdiction of the competent courts in the District of Tel Aviv (the place of residence of the Tender Committee on behalf of the Directorate) in anything relating to and arising out of this Agreement. This Agreement shall be governed by the laws of the State of Israel.

25. **Miscellaneous**

25.1. This Agreement is subject to the provisions of the Budget Foundations Law 5745-1985.

25.2. This Agreement exhausts everything agreed between the parties hereto; any prior agreement or arrangement that were made prior to and until the signing of this Agreement is null and void.

And in witness hereof the parties are hereby undersigned:

The Vendor	**The Directorate**

Appendix C – Data processing

1. Protected data

1.1. Without derogating from the obligations of the Vendor in any other place, the Vendor shall be responsible for guarding, protecting and maintaining the integrity of the protected data in its systems and the Vendor shall not access this data, shall not permit another to access this data, shall not make any use or change in this data and shall not permit any use or change, whether by way of an act and whether by way of an omission, that is not permitted under the provisions of the Israeli law and in accordance with the provisions set forth in the Agreement and this Appendix.

1.2. The Vendor shall be responsible for ensuring that the clients and the users will have regular access to the protected data, in accordance with its obligations set out in this Agreement, and in any event the Vendor shall not deny from them access to the said data, in a manner that is in contradiction to the provisions of the Agreement or the Israeli law.

1.3. The Vendor understands that the protected data includes information regarding the work processes of the Government of Israel and data that is partly related to the citizens and the residents of the State of Israel. Accordingly, any exposure, harm, damage, denial of access, loss of protected data or exposure of data to a third party that might cause to the Tender Holder, to the clients and the users, and to other third parties, serious losses, and shall be obligated to protected the protected data according to the highest standards existing in the market, and not transfer it to any third party in accordance with the provisions set forth in this Appendix.

1.4. Protected data shall not be kept in a public cloud infrastructure other than a cloud infrastructure of one of the cloud providers who won the NIMBUS Tender.

1.5. The obligations of the Vendor with relation to the protected data shall apply as long as the data is stored in its systems, even after expiration of the term of engagement.

1.6. The Vendor shall permit the storage and full documentation of any access and use made by the client and its users to the different Services.

1.7. The Vendor shall have the option to save the documentation for a period of at least one year in such manner that it will be available continuously to the client and to the tender holder.

2. Content data

2.1. The clients shall be entitled to produce content data in the Vendor's systems or by the Vendor's systems, and migrate to the Vendor's systems in the cloud any content data that the clients will deem as necessary, subject to the provisions set forth in any law, including content data under different sensitivity levels, including content data of clients that are subject to different limitations by operation of the law, and the Vendor shall have no claim and shall not impose any limitation in connection therewith.

2.2. In accordance with the Israeli law applicable to the content data of some of the clients as updated from time to time, there are requirements with respect to the protection of the data against its disruption, alteration, or unauthorized exposure. The laws that apply to the data include, *inter alia*, the Security in Public Bodies Law, 5758-1998, the Commercial Torts Law, the State Property Law, and specific laws governing the operations of the State and the civil servants in different areas. The obligations with relation to the protected data under any law are imposed solely on the clients, who are the owners of the data, and not on the Vendor, however only and unless otherwise stated expressly in the Tender documents. The Vendor is obligated to make any reasonable effort for the purpose of allowing the clients and the Tender Holder to meet the different obligations applicable to them under any law with relation to such protected data as said. The provisions of this section shall not derogate from any obligation applicable to the Vendor under any law.

3. Use of the protected data

3.1. The Tender Holder and the clients are the exclusive owners of the protected data and the Vendor shall be deemed as the processor of the protected data and the Vendor shall not make any action in the protected data including storage and saving of the data, its processing and transfer to any third party,

however only in accordance with the provisions of the governing law in the State of Israel and in accordance with the following instructions:

3.1.1. For content data – with the client's approval, according to a digital instruction, and for the regular supply of the services that were purchased.

3.1.2. For processing data – in the required minimal level for the normal supply of the services that are purchased within the framework of the Agreement, including improvement of the cyber protection of the Vendor's systems or the Services, the amounts charged in respect whereof and the performance of the obligations of the Vendor in accordance with the Agreement. It is emphasized that the use of the processing data for the purpose of improving the Vendor's Services that is not part of the improvement of the said Services for the clients, *inter alia*, is prohibited, unless the Tender Holder grants its written approval in connection therewith.

3.1.3. For subscription data – in the required minimum level for the regular supply of the Services that are purchased within the framework of the Agreement, the amounts charged in respect whereof and the performance of the obligations of the Vendor in accordance with the Agreement.

3.2. Without derogating from the foregoing, the Vendor undertakes to keep the data for the periods of time as stated hereunder:

3.2.1. Content data – a minimum of 12 months. The data will be kept for a longer period only after the provisions set forth in section 1.12.1.1 have been fulfilled.

3.2.2. Processing data and subscription data – 90 days, unless the client gives a digital instruction to extend this period of time.

3.3. Without derogating from the foregoing, and for the avoidance of doubt, the Vendor will not sell, lease, or perform any other commercial transaction in the protected data, and in this regard will not transfer the data to another after processing, transferring, or selling the data as part of the data of other users after the erasure of identifying information, or in any other

constellation, without obtaining the prior and written approval of the Tender Holder.

3.4. The Vendor shall not store protected data in its systems in contravention of the provisions set forth in the Agreement and in this Appendix, and in accordance with a digital instruction, and will ensure that such data that is stored in its systems will be disposed, in accordance with the provisions set forth in any law.

3.5. Without derogating from the obligations of the Vendor, the Vendor shall apply the necessary precautions for the purpose of ensuring that the access to protected data is granted only to authorized entities on behalf of the Vendor that require such access to the data for the purpose of providing the Services to the clients. The Vendor is required to ensure that the exposure and the use of the protected data to the authorized entities shall be in the minimal level required for the purpose of providing the service regularly, and according to the obligations imposed on the Vendor. The Vendor shall train the authorized entities regarding the purposes of the use of the data, and the obligations imposed on them in accordance with the law and the provisions set forth in this Agreement as a result of the exposure to such data.

3.6. Erasure of protected data

3.6.1. In 30 days as of the date of receiving the client's request, or in 90 days as of the termination date of the engagement, for any reason, the Vendor shall deliver to the client the entire data of the client, unless the client announced that it was not interested in the data. To the extent that the service allows the client to recover data or erase it directly, the Vendor shall permit the client to perform the said action in 30 days as of the expiration date of the engagement and the Vendor shall provide reasonable technical assistance in the recovery of the data and its erasure and will present to the client proof that the entire data was indeed recovered or erased as required. The entire data shall be recovered in a standard, updated and non-proprietary format.

3.6.2. 90 days after the expiration date of the engagement, or according to a digital instruction demanding the erasure of data and according to the terms of the service, the Vendor shall erase fully the entire

copies of the content data in its systems or in the Services environments in a manner that will not enable their recovery, unless otherwise stated in this Agreement.

3.6.3. Further to the aforesaid, and subject to its obligations under any law, the Vendor shall erase from its records and databases any processing data and subscription data that are not necessary for the purpose of performing the actions permitted under this section.

4. Confidentiality

4.1. The parties agree that the protected data is confidential and may not be used contrary to the provisions of the Agreement, or transferred to any other entity without obtaining the prior and written approval of the Tender Holder.

4.2. The Vendor undertakes to keep in confidence security tools including encryption tools such as stamps and encryption keys that the Vendor provides to the client, and not to provide to any other party any tools or technological assistance in decoding the security tools without obtaining the prior and written approval of the Tender Holder.

4.3. Without derogating from the foregoing, the Vendor shall be obligated to apply all measures required from it for the purpose of keeping in confidence the subscription data and the processing data that are saved in the Vendor's systems in a confidential and secure manner, and in this regard the Vendor undertakes that:

4.3.1. This data shall be protected by the most advanced technological measures existing in the market (state-of-the-art).

4.3.2. Access to these data by the employees of the Vendor shall be made only by authorized persons who require such access and only in the required minimal scope.

4.4. The Vendor shall be held liable for ensuring that secondary processors on its behalf who will receive from the Vendor access to protected data for the performance of the Services to the clients shall be bound by the confidentiality obligation set out in this Appendix and in any event the

Vendor shall be held solely liable for any of their violations of this obligation.

5. Privacy

5.1. Without derogating from its obligations in the Tender and in the Agreement, the Vendor undertakes to act in accordance with the provisions of the Protection of Privacy Law 5741-1981 (hereinafter: the "Protection of Privacy Law") and the regulations enacted thereunder, and any other legislation under Israeli law in connection with privacy under Israeli law for the purpose of enabling the clients to upload personal data that is subject to the relevant legislation (hereinafter: "Personal Data") to the cloud. For the purpose of this matter, it is emphasized that different clients hold different types of rights of Personal Data in different sensitivity levels, for example "medical data," as defined in the Patient Rights Law 5756-1996, personal data, etc.

5.2. With regard to an Israeli service, the Vendor shall not remove Personal Data from the territory of the State of Israel however only after receiving a digital instruction from the client or after obtaining the prior and written approval of the Tender Holder and under conditions that the Tender Holder will see fit.

5.3. With regard to a non-Israeli service, the Vendor shall not remove Personal Data from the territory of a region that is within the EU and the UK and the rules of the General Data Protection Regulation (GDPR) shall apply thereto.

5.4. Without derogating from the obligations of the Vendor, the Vendor shall keep protected data that is under its technological control, such as processing data or subscription data in accordance with the provisions of the law and in particular in accordance with the provisions of the Protection of Privacy Law and the regulations enacted thereunder.

6. Criminal prohibition on the exposure of protected data

6.1. The exposure or disclosure of confidential information in accordance with this Agreement, whether by way of an act or omission not in accordance with express and written authorization of the Tender Holder, constitute

breach of the duty of confidentiality imposed on the Vendor under this Agreement, and constitute a criminal offense, pursuant to section 118 of the Penal Law 5737-1977.

6.2. In addition, and based on the type of the data that was exposed, the disclosure of protected data, whether by way of an act or omission, not in accordance with the provisions of the Agreement or the provisions of the law, might constitute a criminal offense under Israeli law, based on the type of the data that will be exposed (for example, Personal Data, data under privilege in accordance with the Israeli law, data that can compromise national security etc.).

7. Israeli Service

7.1. The content data shall be fully stored within the territory of the State of Israel, unless otherwise stated in this Agreement.

7.2. Content data that is within State of Israel shall not be removed outside the territory of the State of Israel for any purpose, including for processing, storage, backup or for the purpose of their transfer to a third party without a digital instruction from the client or after obtaining the prior and written approval of the Tender Holder and under conditions that the Tender Holder will lay down.

7.3. If the Vendor removed protected data outside the territory of the State of Israel, the Vendor shall erase the protected data immediately, and to the extent that such action was performed for the purpose of providing a service in accordance with a digital instruction, immediately after the completion of the action, in accordance with the terms set forth in the digital instruction and subject to the provisions set forth in any law.

7.4. In any event, the Vendor shall not keep protected data in a state that does not maintain diplomatic relations with the State of Israel.

7.5. The provisions set forth in this section shall apply to a service operating in an overseas region, *mutatis mutandis*.

8. Governing law and jurisdiction over protected data

8.1. Without derogating from the provisions of section 24 of the Agreement:

8.1.1. The State of Israel has full and exclusive sovereign interest and full authorities and rights of ownership in the protected data. As such, the law governing the protected data shall be the laws of the State of Israel and the courts in the State of Israel shall have exclusive jurisdiction over any question or proceeding in connection with the said data, without qualifications or exclusions.

8.1.2. The Israeli law shall govern any direct dispute between the Vendor and the Tender Holder in connection with the protected data, and the courts in the State of Israel shall have exclusive jurisdiction over any question or proceeding in connection with the said data, without qualifications or exclusions.

8.2. The Vendor shall notify immediately regarding any changes or updates in the legal status applicable to the Vendor, that affects the performance of the obligations and the rights in connection with the protected data under this Agreement. For the avoidance of doubt, such a change as said shall not release the Vendor from its obligations in accordance with the provisions set forth in the Agreement.

9. Unlawful transfer of data

9.1. Notwithstanding the provisions of section 8.1, if the Vendor received a request or an order by a foreign entity for the purpose of obtaining protected data, its erasure, alteration, or denial of access thereto, and the Vendor is of the opinion that the request or the order as said are legally binding on it, whether or not the data is within the State of Israel, the Vendor shall act in accordance with the following provisions:

9.1.1. The Vendor shall notify regarding the request or the order to the Tender Holder and the relevant client at the earliest opportunity, and shall update them regarding the steps that the Vendor performed until that stage, unless the Vendor is expressly prohibited by law from acting in such manner as said.

9.1.2. To the extent that there is a gag order on the mere data request, the Vendor shall act for the purpose of lifting this order, and for notifying the Tender Holder regarding the mere existence of the request.

9.1.3. The Vendor shall refuse to transfer the data, and shall raise all legal claims that are relevant, including that the data is the property of a sovereign state and that the data is subject to state immunity.

9.1.4. If necessary, the Vendor shall file an appeal on the decision with the relevant competent court or the administrative authority, and until exhausting all possible appellate options, and shall file an application to stay the execution until a final decision on the subject is made.

9.1.5. According to the request made by the Tender Holder, the Vendor shall request to add the State of Israel as a relevant party to the proceeding.

9.1.6. The Vendor shall take measures for the purpose of reducing the scope of exposure of the data solely to the data that is relevant to the request.

9.1.7. The Vendor shall demand that the requirements made in the request or the order shall be observed in accordance with the instructions set forth in mutual legal assistance treaties and shall not act in accordance with the instructions set forth in the request or the order unless this is possible under the law in the place where the protected data is situated.

9.2. In addition to the aforesaid, if the Vendor received a request or an order by a foreign entity for the purpose of obtaining protected data held in the State of Israel, and the Vendor is of the opinion that the said order is legally binding on it, in addition to the provisions set forth in section 9.1, the Vendor shall act as follows:

9.2.1. The Vendor shall act in accordance with the provisions set forth in the Israeli law for the purpose of enforcing the order (for example,

in accordance with the provisions of the Foreign Judgments Enforcement Law, 5718-1958, the International Legal Assistance Law 5758-1998 etc.).

9.2.2. In any event, the Vendor shall not enforce an order that was issued by an organ of a foreign country on protected data of the Government of Israel that is within the State of Israel, if such an action is not permitted under Israeli law.

9.3. Without derogating from the obligations of the Vendor in any other place, the provisions of this section shall apply to the Vendor even if the request is made from a foreign entity and was received by a secondary processor or another subcontractor operating on behalf of the Vendor for the purpose of performing the Services under the Agreement, and that possesses the protected data. In such circumstances as said, the Vendor shall step in and take over the processor or the subcontractor and shall act according to the said obligations.

9.4. To the extent that the Vendor has an indication that such a request or an order is expected to be received in accordance with the provisions of sections 9.1 and 9.2 above, the Vendor shall notify the Tender Holder about the said forthwith, unless there an impediment by law prohibiting the Vendor from acting in such manner.

9.5. Required actions in the event of transfer of protected data

9.5.1. Without derogating from the liability of the Vendor under any law, and without diminishing from its obligations under this Agreement, in any event in which the Vendor transferred protected data to a third party that is not authorized to obtain the data in accordance with the rules set forth in the Tender, for any reason, including as a result of a request or an order issued by a foreign entity, the Vendor shall act as follows:

9.5.1.1. The Vendor shall notify the Tender Holder at the earliest opportunity regarding any protected data that the Vendor provided as said, the scope of the data, the identity of the data recipient, the reasons for the provision of the data, whether the data was encrypted or protected by other security tools, and any other

relevant information, unless the Vendor is prohibited by law from performing such actions.

9.5.1.2. The Vendor shall not perform any action that can assist in the decoding or the elimination of any technological barrier from protected data in any manner and form, whether by way of an act or omission. If a request as said was received from a law enforcement authority or a security authority of a foreign state for decoding or for making accessible protected data, the Vendor shall contact the Tender Holder and request its approval for the purpose of providing such assistance as said, and shall act in accordance with the instructions of the Tender Holder.

9.5.1.3. If the protected data was transferred without notifying the Tender Holder (whether an order prohibiting the mere disclosure of the demand to transfer the data was issued, whether this is a demand of a security authority and whether for any other reason) the Vendor shall pay to the Tender Holder special damages in the amount of ILS 10,000 within a period of 24 hours from the time the data was provided.

9.5.2. The provisions of this section shall not derogate from the liability of the Vendor and its obligation by law and in accordance with the provisions of the Agreement not to disclose protected data without obtaining the prior and written approval of the Tender Holder and shall not derogate from any right to damages, indemnity, or any other remedy that the Tender Holder may seek in accordance with the provisions set forth in the Agreement.

Appendix D
Security confirmation and confidentiality statement

1. This Appendix constitutes an integral part of the Agreement made between the National Cyber Directorate (hereinafter: the "**Directorate**") and the winning vendor in the Tender (hereinafter: the "**Vendor**").

2. A precondition for the coming into force of the Agreement and the commencement of the engagement is obtaining the approval of the Security Division in the National Cyber Directorate (hereinafter: the "**Security Division**") in accordance with the provisions set forth hereunder, and any deviation from the instructions set forth in this document shall require the approval of the Security Division.

3. Within the framework of the engagement the winning vendor is required to implement all security instructions that are presented in the terms set forth in the Tender, in the Agreement and in this Appendix.

4. Based on the changes or the additions in the Services that the Vendor provides to the Directorate, there might be changes or other/additional security demands that the Vendor shall be obligated to implement fully.

5. The Security Division shall be entitled to conduct audits in the Vendor's offices at any time and by appointment with the Vendor, for the purpose of assuring the implementation of the security instructions applicable to the Vendor.

6. In general, information pertaining to the details of the users of the service, or the details of use that the Directorate makes with the service, and any information related to Tender specification, the scopes of the services, data in connection with the services, search reports and queries, and third-party systems that the Directorate uses (hereinafter: "**Information Related to the Service**") are classified as "**unclassified – sensitive**." The meaning is that these content items are not public and exposure of information related to the engagement and to the Services provided within the framework of the Tender to unauthorized parties might cause harm and/or damage to the Directorate and/or to the entities guided by the Directorate and/or to additional entities, and therefore:

   6.1. The Tender specification may be inspected and used by the Bidders in the Tender and the winning bidder only.

6.2. The winning bidder is prohibited from transferring and sharing Information Related to the Service in any form, including by papers/records, email, attached files, database, sharing by verbal communication etc. to unauthorized entities (an authorized entity is an entity whose information was provided and approved pursuant to the provisions of section 18 hereunder) except for circumstances in which the Vendor obtained prior and written approval from the entity in the Directorate that conducts the engagement with the Vendor and whose information was provided to the Vendor after signing the Agreement (hereinafter: the "**Contract Manager in the Directorate**"). To the extent that such communication of information is approved, the Vendor shall be obligated to deliver a copy of the information that was transferred to the Contract Manager in the Directorate.

7. The Vendor will assure to protect the confidentiality of the information in connection with the engagement from any entity that does not require such information, including the employees and managers of the Vendor in any rank.

8. The entire Information Related to the Service will not be exposed and/or accessible in any manner to other customers of the Vendor.

9. The Directorate shall be solely entitled to decide and select the entities with which it will share any type of information within the framework of the engagement.

10. The Vendor declares that it is aware that the appendix containing the bid in the Tender documents contains sensitive information and the Vendor undertakes to keep in confidence the information that it received from the Directorate and/or that was created and/or that the Vendor holds and/or that will reach its possession and/or to its workers and/or to anyone acting on its behalf during the participation in this Tender.

11. The Vendor undertakes to observe the duty of confidentiality and keep in confidence the sensitive information under safe conditions, and not copy, inform, communicate, or disclose them to any person.

12. In the event that the Vendor is interested in sharing or transferring parts of the scopes of work to subcontractors, the Vendor is required to provide the information of the subcontractors and obtain the approval of the Contract Manager and the Security Division.

13. The Directorate shall be entitled to approve or reject any employees and/or anyone else acting on behalf of the Vendor and to whom the Vendor wishes to provide sensitive information that is related to the Service, without giving reasons.

14. The Vendor is prohibited from advertising the fact that it maintains an engagement with the Directorate. In addition, the mere fact that the Vendor won the Tender shall not be made public by the Vendor or the National Cyber Directorate.

15. The Vendor declares that it read the Penal Law 5737-1977, and in particular sections 117-119 thereof, and the provisions of any other law pertaining to the provision of information and the duty of observance of official information, and it fully understands the nature of the obligation imposed on it by virtue of this undertaking and the fact that it is a contracting party with the Office, and the Vendor shall keep in confidence any information that reaches its possession in connection therewith, and observe the duty to withhold any information without any legal authority to a person that was not authorized to receive such information. In addition, the Bidder declares that it is aware that if it fails to perform this undertaking and/or any of the provisions set forth in the said law, it shall be liable to statutory penal action.

16. For the purpose of obtaining the approval of the Security Division, the Vendor shall deliver a detailed list of names of the persons who will act on its behalf and/or for it, including the workers of the subcontractors who will act for the purpose of performing the activity in accordance with the Tender and the contract.

17. The Security Division shall be entitled to order the Vendor, at any given time, to terminate the employment of any worker who was approved for work in the activity in accordance with the Tender and the Agreement.

18. The following are the persons in the Company that will participate in the engagement and that will be exposed to the information of the Directorate within the framework of the engagement, after obtaining the approval of the Directorate:

No.	Family name	First name	ID. No./Passport No.	Mobile phone	Email
1					
2					
3					
4					

5					
6					
7					
8					
9					
10					

Appendix D – Undertaking of Confidentiality

Entered into and executed in _____ as of this ___ day of _____ 20__

By the authorized signatories on behalf of: _____ (hereinafter: the "Vendor")
Names of signatory(s): _____
ID. No. _____
Address of corporation: _____

Whereas an Agreement was signed between the National Cyber Directorate (hereinafter: the "Directorate") and the Vendor, according to which the Vendor shall provide services to the Directorate, as stated in the Agreement that was signed between the parties;

And whereas: the Vendor might be exposed to professional secrets and the data that the Directorate is interested to protect;

Therefore, the Vendor undertakes towards the State of Israel as follows:

Definitions

In this Undertaking the following terms shall have the meaning set forth beside them below:

The "Services" – the services that are provided within the framework of the agreement that was signed after publication of competitive procedure no. ___ for a cloud-based service (SaaS) for the purpose of analyzing an attack surface, vulnerability management and risk assessment.
"Employee" – each of the employees of the Vendor that will provide the Services to the Directorate.
"Information" – any information, know-how, knowledge, document, correspondence, plan, data, model, opinion, conclusion, information security procedures and physical security, and any other thing connected to and/or relating to the performance of the Services, whether written and whether verbal, and/or in any other manner of saving information in an electrical and/or electronic and/or optic and/or magnetic and/or other manner.

"Professional Secrets" – any information that will reach the Vendor or anyone acting on its behalf in connection with the Services, whether received during the performance of the Services or thereafter, including but without limiting the generality of the foregoing: information that the Directorate and/or any other entity and/or anyone acting on its behalf will provide.

Undertaking of confidentiality

The Vendor undertakes to keep in strict confidence the mere existence of the engagement and the Information and/or the Professional Secrets and use them solely for the purpose of providing the Services subject matter of this Agreement. This shall be done for security reasons, *inter alia*.

For the avoidance of doubt, and without prejudice to the generality of the foregoing, the Vendor undertakes not to publish, transfer, notify, convey, or communicate to any person the Information and/or the Professional Secrets.

I declare that I am aware that failure to perform my obligations constitutes an offense pursuant to Chapter E (Official Secrets) of the Penal Law 5737-1977.

I declare that the Vendor is aware that the disclosure of Personal Data that reaches its possession to an unauthorized entity might also constitute invasion of privacy of a person, an offense liable to legal action pursuant to section 5 of the Protection of Privacy Law 5741-1981.

And in witness whereof I am hereby undersigned:

Date	Name	Stamp of Corporation

Confirmation of attorney

I, the undersigned, _____ Adv., confirm that on _____ Mr./Mrs. _____ who identified himself/herself by ID. No. _____/whom I know in person, appeared before me, in my office in _____ St. in the town/city of _____ and after I warned him/her that he/she is required to declare the truth, and that his/her failure to do so shall subject him/her to statutory penalties, he/she confirmed the truthfulness of this Affidavit and signed it in my presence.

_____	_____	_____
Date	Stamp and License No.	Signature and Stamp

Appendix E – Model Digital Guarantee

Digital guarantee printout

This document is a printout of the digital guarantee and is intended for illustration purposes only – the determining version is the version of the guarantee issuer
This printout was issued by the system of _____ (name of guarantee issuer/guarantee recipient, as the case may be) On DD/MM/YYYY at HH:MM:SS based on a digital guarantee file.

Guarantee information

Digital guarantee code: _____

Guarantee issuer:

_____ branch no.: _____

Telephone number of guarantee issuer: _____ Fax number of the guarantee issuer: _____

Address of guarantee issuer: _____

Street and number: _____ City/town: _____ Zip code: _____

Name of authorized signatory 1: _____

Name of authorized signatory 2: _____

Guarantee recipient:

_____

_____

The debtors (hereinafter jointly and/or severally: the "Debtor"):

Debtor Identification	Debtor Name
_____	_____

Subject matter of Guarantee:

(Name of Tender/subject matter of engagement)

Amounts and dates

Guarantee amount _____ new Israeli shekels.

Linkage: _____ without linkage

Guarantee issue date: _____ (this part will be completed by the issuer), guarantee expiration date: _____

Undertaking wording

The guarantee issuer hereby guarantees towards the guarantee recipient, for the Debtor, the settlement of any amount that the guarantee recipient will demand from the guarantee issuer in connection with the subject matter of the guarantee, and that will not exceed the guarantee amount. The guarantee issuer hereby undertakes to pay to the guarantee recipient the said amount within the number of days for forfeiture set out in this guarantee, as of the date of receiving the demand of the guarantee recipient and the guarantee recipient shall not be obligated to give reasons for his demand or demand first the settlement of the amount from the Debtor.

In the event of such a demand as said, the guarantee issuer shall not invoke any defense claim against the guarantee recipient that it or the Debtor may invoke, and shall not stipulate the payment on any conditions or delay the payment for any reason, including the settlement of the said amount from the Debtor.

This guarantee is nontransferable and non-assignable.

This guarantee may be realized in installments in such manner that its partial forfeiture shall not derogate from its effect with respect to the balance of the guarantee amount that was not forfeited, and provided that the total payments under this guarantee shall not exceed the guarantee amount.

This guarantee shall be governed solely by the laws of the State of Israel.

The rules for the purpose of handling this guarantee shall be in compliance with the digital guarantees standard as published in the website of the TAKAM Regulations of the Accountant General, according to their wording on the guarantee issue date, including in accordance with the following rules:

1. This guarantee shall be managed digitally, by delivery of demands and requests between the systems of the guarantee recipient and the systems of the guarantee issuer, in accordance with the rules set out in the digital guarantees standard.
2. The dates in the guarantee refer to calendric days, ending at 23:59, except for the count of days for payment in respect of the forfeiture of the guarantee by the guarantee issuer. The count of days for payment in respect of forfeiture of the guarantee shall commence on the banking business day in which the demand for forfeiture was received from the guarantee recipient. In the event that the demand was received not on a banking business day, the count of days for the performance of the forfeiture shall commence on the subsequent bank business day.
3. After the expiration date of the guarantee lapsed, the guarantee shall expire and the Debtor, the guarantee recipient or the guarantee issuer shall not be required to perform any additional action.

Number of days for forfeiture: 15

References (to be filled by the technological system, not by the Ministry)

Internal reference of the guarantee issuer: _____

Internal references 1 of the guarantee recipient: _____

Internal references 2 of the guarantee recipient: _____

Internal references 3 of the guarantee recipient: _____

Internal references 4 of the guarantee recipient: _____