Ministry of Finance – Accountant General's Department

Government Procurement Administration

"Nimbus Project"

Central Tender 01-2022 for the addition of services to the Government Cloud Marketplace

Booklet no. 1: Tender Documents

Version ~~1 – June~~2 – September 2022[1]

[1] *The English version of the Tender is published for the convenience of interested suppliers only, and is not the legally binding version of the Tender documents. The Hebrew version of the documents is the formal version, and will take precedent over any other document.*

Introduction

The Government Procurement Administration in the Accountant General's Department of the Ministry of Finance (hereinafter: **the Tender Administrator**), hereby publishes Central Tender No. 01-2022 **on the topic: adding services to the government digital marketplace in the cloud** (hereinafter: the "**Tender**").

This Tender is part of the Nimbus Project, a multi-year project, intended to give a comprehensive, in-depth response to the provision of public cloud services for government ministries, auxiliary units and related bodies (hereinafter: the "**Clients**"). As part of the Nimbus Project, and in accordance with the various layers of the project, the companies Amazon Web Services EMEA Sarl (hereinafter: "**AWS**") and Google LLC (hereinafter: "**GCP**") (hereinafter, together: the "**Cloud Providers**") won Central tender 01-2020 for the provision of cloud services on a public platform for the government ministries and auxiliary units (hereinafter: the "**Cloud Tender**"). The Cloud Providers are establishing, each by itself, a public cloud region in the State of Israel.

The purpose of this Tender is to provide Clients with third party services from the Cloud Providers' service catalog (marketplace), beyond the services offered by the Cloud Providers themselves, so that these services will be available in the government digital marketplace for the Clients (hereinafter: the "**Tender**").

In addition to the Government Digital Marketplace, the Government will establish additional digital marketplaces for dedicated client groups with increased information security requirements (hereinafter: "**Specific Digital Marketplace**"). The bid of bidders whose bid for the Government Digital Marketplace has won will be examined for their suitability for a Specific Digital Marketplace, in accordance with the specific rules set in relation to that particular Specific Digital Marketplace.

Bids for this Tender may be made periodically in accordance with the dates to be determined by the Tender Administrator, where each bidder may offer any of the services that it wishes to include in the government digital marketplace or in a Specific Digital Marketplace for the Clients.

The RFP documents are divided into chapters, as set forth below:

Chapter ~~1~~1 – the Tender procedure, for enrolling in the digital marketplace.

Chapter 0 – the bidding booklet, which will be submitted by the bidder participating in the Tender. *This chapter is published separately*.

~~Chapter 3~~Chapter3 – the engagement agreement.

Professional Definitions

Region – A defined geographical region, which includes one country, part of one country or a defined supranational entity (such as the EU), which includes at least one zone from which cloud services are provided to customers by a cloud service provider.

Overseas region – the public region proposed in the bid of the winning providers of the cloud tender – for AWS, the Ireland region (eu-west-1) and for GCP, the Netherlands region (europe-west-4) and in addition Frankfurt region (~~europe~~Europe -west-3).

Israeli region – a public region that will be established by the Cloud Providers in the territory of the State of Israel and which meets the requirements set out in the cloud tender and as set forth in the winning bid for the cloud tender.

Public region – a region from which public cloud services are provided by the cloud service provider, and which is connected to the global public cloud infrastructure operated by the cloud service provider (other regions operated by the Provider worldwide), but it (and the zones located in it) may be operated separately from any other region that the cloud services provide operates worldwide.

Security incident – an incident that may impair the availability, integrity or confidentiality of protected information or the services used by the Clients, including a cyberattack.

Tender Page – the tender page on the website of the Government Procurement Administration at www.mr.gov.il, where all the information regarding the tender, including the tender documents and all related notices and announcements, will be published.

Digital instruction – An instruction given using a customization and configuration tool such as the Provider's management interface, APIs or any other means made available to the Client.

Enterprise customer – a ~~business, governmental or public~~ customer that has at least 50,000 or above users.

Protected information – processing data, access data and content data.

Cloud tender – Central tender 01-2020 for the provision of cloud services on a public platform for the government ministries and auxiliary units

Sub-processor – a subcontractor that the Provider engages with and for which it performs protected information processing.

Provider systems – computing infrastructures that operate on public cloud infrastructures, or anywhere else, and which are used by the Provider to provide the services to the Clients.

Zone (Domain / Availability Zone) – a defined location within a specific region, which includes at least one data center (different zones will not share the same data center) from which cloud services are provided to customers. Each zone has cooling resources, network connections and power supplies that are completely separate from those of any other zone and is connected to every other zone in the same region via quick links.

Access data – any information of users and Clients that the Provider needs for the purpose of managing access, providing services or for billing.

Processing data – any information that is generated in the Provider's systems during or as a result of processing of content data (metadata and logs), which is attributable in any way to a Client, a group of Clients or a user including user identification and details (including name, address, billing information, date of birth, email address, telephone number), system login and logout dates and times, information on Clients, services that they run, configuration data and files, the actions performed in the various systems, usage details, IP addresses assigned by service providers (access data), transactional data and traffic data, including geolocation of the source and destination of the data, data size, data structure, route, communication protocol.

Content data – the digital data, including any information, file, database, software, code, logic, data entry, report, mark, text, image, audio, video, photo, etc. in any format, which has been uploaded, created directly by or at the request of a user in the Provider's systems, including the third-party services used by the Provider.

Cloud Providers – the companies Amazon Web Services (AWS) and Google, which have won the cloud tender.

Information processing – an action or series of actions performed on information, whether by automatic means or not, such as collection, recording, organization, construction, storage, transfer, adaptation or modification, retrieval or restoration, usage, encryption, distribution or setting up for viewing in any other way, alignment or combination, restriction, deletion or destruction and so on.

~~**Public Cloud** – Cloud services provided on the basis of a cloud provider platform, and which are commercially available and used by various customers, including individuals, companies and corporations, government bodies and others.~~

Public Cloud – cloud services that are provided on the Cloud Providers' platform, and are available and are used by different clients for commercial purposes, including individuals, companies and corporations, government entities ~~etc. ~~and others.

Third party – a legal entity that is not owned or controlled by the Cloud Provider that has won the cloud tender.

Subcontractor – a third party through which the Provider meets some of its obligations in accordance with this Tender.

Category – a list of services in a particular field (for example: security, CRM, Backup & Recovery, etc.) offered for sale in the Cloud Provider's marketplace.

Marketplace – a list of all the applications, services and other tools offered by the Provider that has won the cloud tender publicly to its Clients. These services can be operated, used and consumed on the Provider's public cloud platform, and are provided by the Provider itself or by a third party.

Subscription – a business model in which a customer purchases a service and pays for it periodically, where the licensing is provided by a third-party service provider through the digital marketplace, which is responsible for allocating the subscription, registration and providing the software or service to the customer~~ using a SaaS or Machine Image model.~~.

Digital marketplace – a virtual store operated by the cloud service provider specifically for the Clients in this Tender, in which the Clients can locate and purchase applications and services offered by the cloud service provider itself, as well as by other companies (third party services), and consume them on the Provider's public cloud services platform.

Central governmental service – a service that the Tender Administrator has chosen as part of a tender procedure as a single solution for a specific area of service for government ministries.

Cloud services – cloud computing services provided to a user by one or more remote computers.

Service provided in the Israeli region or Israeli service – a service wholly provided from the Israeli region of one of the Cloud Providers, in which all processing, traffic and storage of~~,~~ content data is performed in the Israeli region only.

Third party services – services that can be consumed by users of the Cloud Provider's public cloud platform, and which are owned by a third party and priced by a third party only, without the Cloud Provider's involvement.

SaaS – Software as a Service – a model for consuming a cloud software service that meets one or more of the following alternatives:

- The service provider deploys and hosts the software on the Cloud Provider's infrastructure and is responsible for providing customers access to the software and services provided in it and maintaining the level of service for customers.
- As part of the service, Clients' content data is transferred, stored or processed in the Provider's systems or systems under its control.
- As part of the service, Clients' content data is kept, permanently or momentarily, under the control of the Provider (including reading, modifying, deleting, performing any other action on the data or changing the permissions to access it).

Software that is not software as a service – Non-SaaS – any service that operates on a cloud providers' cloud platform and is not software as a service (SaaS).

Commitment-based pricing – a model for purchasing a service or software with a subscription in which the customer purchases a quantity or usage scope in advance (including purchasing using a commit, RI model or as part of installment payments).

Consumption-based pricing – a model of purchasing a service or software with a subscription where the customer pays for the service according to the actual consumption of the service or software.

Cyberattack – a security incident that aims to pass or bypass the security or control measures used by the Provider or Client or exploit an existing vulnerability in an attempt to cause disruption of the service or destruction, loss, leakage, alteration, use, unauthorized disclosure or access to Protected information.

Service Level Agreement (hereinafter: "**SLA**") – an agreement between a service ~~provider~~Provider and an end user that defines the level of service expected of the service ~~provider~~Provider and prescribes compensation for deviation from this level.

1. Chapter 1 – The Tender Procedure for Enrolling in the Digital Marketplace

1.1. General

1.1.1. This Tender is a public central tender published in accordance with the Mandatory Tenders Regulations, 5753-1993 (hereinafter: the "**Mandatory Tenders Regulations**").

1.1.2. The Tender is for the purpose of entering the Government Digital Marketplace in the cloud, as well as for Specific Digital Marketplaces, as set forth in the tender documents.

1.1.3. The inclusion of services in the digital marketplace will be in accordance with the categories of services set forth in the marketplace of the Cloud Provider, as will be updated from time to time.

1.1.4. The Tender Administrator will update, from time to time, the categories for which bids in the Tender may be submitted and will determine the closing date for each category.

1.1.5. A bidder that is interested in submitting a service in a certain category will submit Chapter 2 – the bid booklet, which will be published for submitting a bid at the relevant time.

1.1.6. A bidder will specify which services it is offering, and in which categories of Cloud Providers the service is being offered in the marketplace. A bidder can submit one or more services in each category. Compliance with the Tender requirements will be examined individually for each service.

1.1.7. As part of the Tender, A Bidder may submit services in SaaS or Non-SaaS configuration only, and deployment and integration services associated with these services, as specified below in the tender documents. It is not possible to submit the sale of the deployment and integration services (such as Professional Services) as a stand-alone item.

1.2. Threshold conditions for submitting bids

1.2.1. A bidder that meets, by the closing date for a given category, the threshold conditions set forth below, is allowed to participate in the Tender.

1.2.2. Proof of compliance with the threshold conditions will be made in accordance with the instructions in the bid booklet (Chapter 2).

1.2.3. **Threshold conditions:**

1.2.3.1. If the bidder is a corporation established in Israel:

1.2.3.1.1. The bidder is legally registered in Israel.

1.2.3.1.2. The bidder complies with the provisions of the Public Bodies Transactions Law, 5736-1976 (hereinafter: the "**Public Bodies Transactions Law**").

1.2.3.2. If the bidder is a corporation established in a country other than Israel (hereinafter: "**foreign country**"):

1.2.3.2.1. The bidder is legally registered in a foreign country that maintains diplomatic relations with the State of Israel.

1.2.3.2.2. To the extent that the bidder is registered in Israel or has an active representation unit in Israel, it complies with the provisions of the Public Bodies Transactions Law.

1.2.3.3. The bidder has the full right to sell the offered service in the governmental digital marketplace under the Tender and to commit to the requirements of the tender.

1.2.3.4. The service being offered is available in the marketplace of one or both of the Cloud Providers.

1.3. Parameters for examining the services being offered

1.3.1. **Each service offered will be required to meet the parameters listed below:**

1.3.1.1. Evaluation of the services – compliance with a minimum score in matters of cyber, privacy protection and other information security aspects, as set forth in the evaluation table in Section 1.3.2 below.

1.3.1.2. Price quotation – the bidder must offer a quotation that will be submitted according to the requirements set forth in Appendix 5 of chapter 2 – bid booklet.

1.3.2. Evaluation of the services

1.3.2.1. Services provided in Software as a Service (SaaS) Model

#	Topic	Minimum	Weight
1.	**Business continuity and SLA** – resiliency configuration, risk management, backup, deployment in different zones.	-	10%
2.	**Protection and securing of processes and infrastructure** – cyber protection systems and security processes, service configuration security, supply chain and human capital protection, tools and processes available to the Client, encryption, compliance with standards, risk management.	-	50%
3.	**Protection of Clients' information** – the ability to separate Clients, the scope and manner of access of support representatives, how the services are linked to the Client's systems, login and authorizations, logs and investigation	-	40%
Total		**80%**	**100%**

1.3.2.2. Services not provided in Software as a Service model (non-SaaS)

#	Topic	Minimum	Weight
1.	**Protection and security of work processes** –service configuration security, supply chain and human capital protection, encryption, compliance with standards, risk management.	-	60%
2.	**Protection of the Clients' information** – the scope and manner of access of support representatives, the scope of the information stored at the Provider and the manner in which it is secured, login and authorizations.	-	40%
Total		**80%**	**100%**

1.3.2.2.1. The Tender Administrator or an agent thereof will score each of the topics listed above, in accordance with an internal document for checking, which will be drafted before the submission of the bids. The Tender Administrator may establish an appropriate internal document for checking for each specific digital marketplace.

1.3.2.2.2. After scoring each of the topics listed in the tables above, the total score of the bid will be calculated (between 0 and 100) by adding up the bids' accumulated points.

1.3.2.2.3. The Tender Administrator set a minimum quality score, in accordance with the type of service, as specified in the table above. A service which will not meet the minimum quality score will be disqualified.

1.4. Announcement of winners

1.4.1. Candidates for winning

1.4.1.1. The Tender Administrator will declare ~~a service that is~~all of the services which were found to meet the parameters listed in the tender documents as eligible services to be available in the digital marketplace (hereinafter: "**Candidate for Winning**"). ~~A~~ A Bidder whose services (or a part of them) were declared as Candidate for Winning ~~is~~, will be required to perform the following actions:

1.4.1.1.1. To enroll in the Government Digital Marketplace and in any Specific Digital Marketplace for which ~~it is~~its services were found eligible, ~~as well~~in accordance with the instructions of the Tender Administrator and the manner of working with the cloud platform of the relevant Provider. For this purpose, the Bidder will be required to implement any technical requirement in the cloud Providers systems required for the purpose of completing the registration and creating the availability of the Candidates for Winning in the Government Digital Marketplace, as ~~signing~~it will be established, including the establishment of a separate registration of the Candidates for Winning in the cloud Providers Marketplace.

1.4.1.1.2. Signing the Service Agreement ~~(Chapter 3), according to the procedure~~(Chapter 3), as specified below:

1.4.1.1.2.1. Signing the Service Agreement in accordance with a process to be defined by the Tender Administrator~~. A bidder may sign~~ , and by the cloud infrastructure on which the services is to be provided.

~~1.4.1.1.1.1.~~1.4.1.1.2.2. 1.4.1.1.2.2 Signing a single Service Agreement for ~~multiple services.~~ all the Candidates for Winning

1.4.1.1.2.3. Signing the service agreement in the official version published by the Tender Administrator in the Hebrew language or in the English language, in accordance with the Bidders choice. If the Bidder choses to sign the English version of the agreement, the agreement in Hebrew will be attached to it as an appendix, which will prevail in any case of contradiction.

1.4.1.1.2.4. The Bidder is entitled to attach to the Service Agreement terms of use for a specific service, in accordance with the provision of section 3.10.5.

1.4.1.2. A Candidate for Winning that completes the process of enrolling in the digital marketplace will be declared as a winner and may offer its services that were declared as Candidates for winning to Clients.

~~1.4.1.3.~~ A ~~Candidate for Winning will be required to implement any technical requirement in the Cloud Providers' systems, required by the Tender Administrator, in order to complete the registration and create availability of its services in the government digital market, including establishing a separate listing of services approved for the government digital market in the Cloud Providers marketplace.~~

~~1.4.1.4.~~1.4.1.3.~~The win of a bidder~~Bidder that does not meet the aforesaid requirements ~~above~~ for ~~some~~part or all ~~services~~of the Candidates for winning, within ~~the~~a time ~~set~~frame to be determined by the Tender Administrator, its winning will be ~~denied~~revoked for those services. Alternatively, the Tender Administrator, in accordance with the sole discretion thereof, may grant the Bidder an extension to complete the required actions.

1.5. Phases and dates in the Tender

1.5.1. The Tender will be conducted according to the schedule set forth below:

Topic	Date
Bidders' Conference	Please review the clarification document regarding the Bidders' conference and the submission of clarification questions and comments, as published in the Tender page
Deadline for submitting clarification questions	
Deadline for the Tender Administrator to answer clarification questions	At least 7 days before the closing date
Closing Date	Will be published from time to time in the bid booklet (Chapter 2), as will be published on the Tender Page

1.5.1.1. The ~~times listed~~schedule detailed in the table obligate all bidders interested in participating in the Tender, whether for categories whose submission deadline has been published or for future categories.

1.5.1.2. The Tender Administrator is allowed, at its sole discretion, to modify the schedule above.

1.5.2. Bidders' conference

1.5.2.1. Bidders ~~must~~should register in advance to participate in a bidders' conference. A link for registration will be published on the Tender Page. The bidders' conference will be held in English, if required.

1.5.2.2. There is no obligation to attend the bidders' conference. It should be clarified that all the information provided at the bidders' conference is intended to clarify the contents of the tender documents and that only the tender documents are binding.

1.5.2.3. It should be clarified that answers given orally at a bidders' conference will not obligate the Tender Administrator. Binding answers will be given only as part of the clarification questions procedure set forth above.

1.5.3. Clarification questions

1.5.3.1. In any case of ambiguity or comments regarding the Tender, its times or conditions, clarification questions or comments should be sent to the Tender Administrator via submission of digital form (link will be posted on the tender page) before the deadline for submitting clarification questions stated above. The time for clarification questions is intended for all submission times, as set forth below in Section 1.6, and subject to the statements in Section 1.5.3.5 below, no additional option for submitting questions will be given.

1.5.3.2. The questions will be submitted using concise, clear wording in Hebrew or English.

1.5.3.3. The Tender Administrator is not required to answer questions that are submitted after the deadline or that asked orally, by telephone or in a format differing from that required.

1.5.3.4. Questions sent anonymously will not be answered.

1.5.3.5. To the extent necessary, the Tender Administrator may allow, in its sole discretion, additional rounds of clarification questions, by publishing a notice on the Tender Page.

1.5.3.6. A bidder that will not ask the Tender Administrator clarification questions about the Tender as stated in this section will be barred from making any argument, demand or claim against the Tender or any of its terms in the future.

1.5.4. The Tender Administrator's answers to clarification questions

1.5.4.1. Answers and clarifications of the Tender Administrator will be given in writing only and will be an integral part of the tender documents. Only written answers and clarifications will obligate the Tender Administrator.

1.5.4.2. Answers and clarifications from the Tender Administrator will be published on the Tender Page. Bidders must study the answers of the Tender Administrator as well as any updates that will be published as set forth in relation to this Tender.

1.5.4.3. The Tender Administrator may make any changes to the tender documents and give an interpretation or clarification to the provisions of the tender documents, regardless of the clarification questions.

1.5.4.4. The Tender Administrator is not bound to the phrasing of a clarification question that has been submitted, and may, when phrasing an answer to a question, shorten the wording of or rephrase a question. The phrasing of the Tender Administrator's answers is the binding wording and constitutes an integral part of the tender documents.

~~1.5.4.5. If deemed necessary by the Tender Administrator, under his full discretion, may allow additional rounds of clarification questions in a notice that will be published on the tender page.~~

1.5.5. Submission of bids for the Tender

1.5.5.1. Submission of bids for the Tender will be done according to instructions specified in chapter 2 – bid booklet.

1.6. Future times for submission of bids for services

1.6.1. In addition to the tender ~~times~~schedule set forth above, the Tender Administrator will publish, from time to time, dates for submitting bids for additional services in additional categories, or addition of services and providers in existing categories.

1.6.2. The list of categories above and the times for submission of bids for services for them will be updated from time to time, according to the following outline:

1.6.2.1. ~~Before each opening of a category/categories, at~~At least 30 days' notice will be given before opening of a category/categories. The notice will be published on the Tender Page and will be sent to a distribution list. Registration for the distribution list will be ~~as set forth on the Tender Page~~in the manner which will be specified in the Tender Page. It should be clarified that the bidder has sole responsibility for monitoring these publications on the tender page.

1.6.2.2. The submission date will be announced at the time of publication of the bid booklet (Chapter 2) for that category, which bidders in that category will be required to submit.

1.6.2.3. At any time, the latest version of the tender documents, the list of categories open for submission and the closing date will be available on the Tender Page.

1.7. The Tender procedure

1.7.1. Bids evaluation

1.7.1.1. The Tender Administrator or a team on its behalf, which may also include external consultants who are not government employees, will evaluate the bids.

1.7.1.2. In addition to the information contained in the bid, for the purpose of evaluating bids, the Tender Administrator or its representative will use professional knowledge available to it, any reliable information sources including public information about the bidder, the experience of the Tender Administrator or one of the Clients, professional consultants' opinions, reports and comparisons by research companies (such as Gartner) and any other reliable source of information.

1.7.1.3. The Tender Administrator may evaluate the bids in any way it sees fit, including by requiring bidders to present the services they offer or any part of them, to give the Tender Administrator a specific user account (for SaaS configuration services) that allows the services to be tested independently in a public region chosen by the Tender Administrator, etc. It should be clarified that all the costs involved in performing the demonstrations, presenting the services or examining the services independently by the Tender Administrator will be at the expense of the bidder. It should be clarified that the Tender Administrator will arrange with the bidder tests that place a considerable burden on the bidder's systems or whose cost is high.

1.7.1.4. The Tender Administrator or its representative may ask a bidder to explain a particular detail of its bid, complete a detail missing from it or submit an additional or alternative document proving its meeting of the Tender conditions, within a specified period of time, or may reduce the bidder's score, depending on the part missing from its bid, at the sole discretion of the Tender Administrator.

1.7.1.5. Without detracting from the powers of the Tender Administrator, the Tender Administrator may:

1.7.1.5.1. Hold a meeting with bidders for the purpose of clarifying the technological, security and operational aspects of the bid.

1.7.1.5.2. Reclassify a service that has been misclassified by the bidder under the wrong category or that has been misclassified by the bidder as a SaaS service and vice versa. In such a case, the Tender Administrator will inform the bidder of the reclassification of the service being offered and will ask it to complete Appendix B in a manner corresponding with the reclassification.

1.7.1.6. Failure to respond to a request for completion or clarification, or failure to respond within the specified time, may result in disqualification of the bid.

1.7.1.7. After the bidder has been given an opportunity to complete and clarify its bid, the Tender Administrator may disqualify a bid that still does not meet the requirements of the Tender, or, at its discretion, may request supplementation or further clarification.

1.7.2. Validity of bids

1.7.2.1. A tender bid will be valid for up to 6 months from the closing date. The Tender Administrator may announce the extension of the bids' validity for additional periods and up to 3 months more in total, for the purpose of making a final decision and selection of bidders to be declared as Candidates for Winning.

1.7.3. Disqualification of bids

The Tender Administrator may disqualify a bid that has been submitted in the Tender, at its discretion, if one of the following conditions applies, among other reasons:

1.7.3.1. **Disqualification of a deficient or unclear bid** – if a bid submitted for the Tender is deficient to such a degree that the Tender Administrator is unable to understand the essence of the bid, or if it lacks clarity or is insufficiently organized.

1.7.3.2. **Disqualification of a bid that is at a loss** – if the bid is not economical to a bidder, to such an extent as to shed doubt as to its ability to meet its obligations, should it win the Tender.

1.7.3.3. **Disqualification of a deceptive bid or a bid submitted in bad faith** – if the bid includes exceptional prices or discounts (dumping prices) etc., both in relation to the bid itself and in relation to other bids and in relation to market prices, or contains misleading information or any other case in which the bid is made in bad faith, including in the case of an action or behavior of the bidder, under the Tender, in bad faith.

1.7.3.4. **Disqualification due to behavior in previous tenders and engagements** – within a previous tender or engagement of the Tender Administrator or a Client, the bidder has acted in bad faith, deceptively, fraudulently or dishonestly, has provided misleading information or material inaccurate information or has acted extremely unprofessionally, in a manner that in the opinion of the Tender Administrator justifies its disqualification.

1.7.3.5. **Disqualification of a bid due to the bidder's financial situation** – if due to the bidder's current or forecasted financial situation, including due to bankruptcy or liquidation proceedings or material claims that have been instigated against it, there is concern as to its ability to comply with its obligations involved in winning the Tender.

1.7.3.6. **Disqualification of a bid due to conflict of interest** – if there is a direct or indirect conflict of interest, or fear of a conflict of interest between the interests of the bidder, the bid that it has submitted, or stakeholders therein and participation in and winning the Tender or the performance of the services by the bidder in a way that the Tender Administrator believes cannot be remedied.

1.7.3.7. **Disqualification of a bid owing to coordination of bids** – if there is reasonable suspicion of coordination between the bidder and other bidders in the Tender, or between the bidder and a potential bidder.

1.7.4. In such cases, the bidder will be given a right of pleading in writing or orally before the final decision is given, subject to the sole discretion of the Tenders Committee.

1.7.5. Cancellation or modification of the Tender

1.7.5.1. The Tender Administrator, on its own initiative and at its discretion, may cancel, modify or update the Tender, including updates of dates set forth in it. Such changes will be announced on the Tender Page.

1.7.5.2. The engagement with the winner of the Tender is subject, among other factors, to the Clients having a budget available for it. If for budgetary reasons it will not be possible to engage with the winner of the Tender, the Tender Administrator may cancel the Tender.

1.7.5.3. The Tender Administrator will not be required to compensate the bidders in the case of cancellation or modification of the Tender.

1.7.6. Appointment of a representative on behalf of the bidder

1.7.6.1. For the purpose of the Tender, the bidder will appoint a representative on its behalf, who will be the exclusive contact person for all inquiries regarding the Tender.

1.7.6.2. Any response or feedback sent by the bidder's representative to the Tender Administrator, ~~or~~will obligate the bidder, and every massage from the Tender Administrator to the bidder's representative~~,~~ will ~~obligate~~be considered as delivered to the bidder.

1.7.7. Expenses

1.7.7.1. The bidder will not be entitled to any reimbursement of expenses or any compensation in relation to the Tender, including in the event of its termination, delay, change of terms or cancellation.

1.7.8. **Applicable law and jurisdiction**

1.7.8.1. The law applicable to any matter related to the Tender is Israeli law, without exceptions or qualifications, and the jurisdiction in all matters and issues relating to the Tender, or in any claim arising from the process of conducting it, will rest exclusively with the competent courts in Jerusalem.

1.7.9. **Confidentiality of the bid and the right of inspection**

1.7.9.1. Subject to the statutory duties of the Tender Administrator, the Tender Administrator undertakes not to disclose the content of a bid that is submitted in this Tender to a third party that is not one of the Tender Administrator's representatives or consultants employed by it for the purpose of the Tender, to which the duty of confidentiality and refrainment from using the bidder's bid will also apply, except for the purposes of the Tender only.

1.7.9.2. In accordance with the Mandatory Tenders Regulations, bidders that have not won the Tender may request to inspect the winning bids, as well as additional documents related to the Tender and the Tender Administrator will only prevent them from inspecting documents that are a trade or professional secret, or which may harm the state's security, its' foreign relations, economy or public safety.

1.7.9.3. According to the nature of the Tender, the part of the bid that is "Appendix 4 to Chapter 2 – unique requirements on cyber protection, privacy and other issues in the field of information security" is defined by the Tender Administrator as a trade or professional secret, meaning that there will be no right of inspection for this part of the bids.

1.7.9.4. If a bidder wishes to prevent inspection of additional sections of its bid due to an assertion of a trade secret, professional secret, or for any other reason mentioned in the Mandatory Tenders Regulations, it must state this explicitly in the tender booklet (Chapter 2). It is clarified that the act of making the request will not prevent inspection of the relevant sections, and a decision on the subject will be made by the Tenders Committee of the Tender Administrator.

1.7.9.5. A bidder that has asserted that a particular part of its bid is a trade or professional secret will be barred from demanding to inspect that part of other bids.

1.7.9.6. In the event that the Tenders Committee of the Tender Administrator rejects a bidder's assertion that parts of its bid are a trade or professional secret, the Tender Administrator will inform it of this at least 5 workdays before the actual right of inspection is enacted.

1.7.9.7. The final decision regarding the certain details of a bid constituting trade or professional secrets, is up to the Tenders Committee, at its discretion.

1.7.9.8. Subject to the provisions of this section, by participating in the Tender, the bidder agrees that its bid will be submitted in its entirety, including all of its appendices, for inspection by the other bidders in the Tender in accordance with the provisions of the law and the Mandatory Tenders Regulations.

2. Chapter 2 - the Bid Booklet

Attached as a separate document.

3. Chapter 3 –

Service Agreement – Nimbus

Between

The Government of Israel on behalf of the State of Israel
By the Government Procurement Administration in the Accountant General's Department of the Ministry of Finance
(Hereinafter: the "**Tender Administrator**")

Party A

And

____

of ____

(Hereinafter: the "**Provider**")

Party B

Whereas The Tender Administrator has published Central Tender No. 02-2022 for Adding Services to the Government Digital Marketplace (hereinafter: the "**Tender**"); and

Whereas The Provider has submitted a bid for the Tender, and subject to its enrollment in the service agreement – Nimbus (hereinafter: the "**Agreement"**) and compliance with the requirements set forth in the Tender and the Agreement, the tenders committee of the Tender Administrator has selected the Provider as a provider available in the Government Digital Marketplace.

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

3.1. General

3.1.1. **The appendices set forth below are attached to this Agreement:**

3.1.1.1. **Appendix A** – the list of services that have been approved for the digital marketplace, as will be updated from time to time;

3.1.1.2. **Appendix B** – the bid booklet of the bidder in the Tender;

3.1.1.3. **Appendix C1** – information processing for services in Software as a Service (SaaS) configuration

3.1.1.4. **Appendix C2** – information processing for services that are not in Software as a Service (Non-SaaS) configuration;

3.1.1.5. **Appendix D1** – security and cyber for services in Software as a Service (SaaS) configuration;

3.1.1.6. **Appendix D2** – security and cyber for services that are not in Software as a Service (SaaS) configuration;

3.1.1.7. **Appendix E** – Hebrew agreement (will only be attached if the English version of the agreement is signed)

3.1.2. The preamble and appendices to the Agreement form an integral part hereof.

3.2. Interpretation

3.2.1. In this Agreement, the terms will have the meaning that appears in the tender documents unless otherwise stated in the Agreement or its appendices.

3.2.2. The Agreement and its appendices will be interpreted in a manner that meets the requirements of the Tender, and in a manner that fulfills the purpose of the Tender for the provision of cloud services to the Government of Israel from the Israeli region, in the best possible way.

3.2.3. In the event of an explicit or implicit contradiction between provisions in relation to the duties imposed on the parties to this Agreement, the following interpretive hierarchy will apply:

3.2.3.1. **Appendix C** "information processing" – the statements therein supersede those made in any other document;

3.2.3.2. The Agreement and its appendices – the statements therein supersede those made in any other document;

3.2.3.3. In the absence of an explicit or implicit provision in the agreement or the tender that contradicts the provisions of the terms of use of a particular service, the terms of use will apply, in accordance with the provisions of section 3.10.5. Notwithstanding the foregoing, a provision set forth in the terms of use of a service which has received an individual approval from the Tender Administrator, as specified in section 3.10.5 of the Tender documents, shall prevail over the provisions of the agreement and the appendices thereof.

3.2.4. In any case of contradiction within the hierarchy set above, between the various professional requirements applicable to the Provider in the same hierarchy (whether these are the requirements set forth in the tender documents or a contradiction between the requirements of the Tender and the Provider's bid), the Provider will act in accordance with the strictest binding level and provision of service in a way that benefits Clients.

3.3. Enrollment in the Agreement

3.3.1. The parties consent and commit to all of the conditions set forth herein. In witness whereof the parties have signed:

The Tender Administrator:	**The Provider:**
Name	Name
Signature	Signature
Name	Name

Signature

Signature

Part A - Principles

3.4. Subject of the ~~Agreement~~Tender

3.4.1. The subject of the ~~engagement~~tender is ~~purchasing~~the regulation of the procurement of services, which are not the Cloud ~~Provider~~Providers' services~~, and are~~ available in the services catalog of the Cloud Providers, ~~and building~~while establishing a digital marketplace for Government ministries and auxiliary units and specific digital marketplaces according to Clients' needs. The following services shall not be considered as part of the tender Subject:

~~3.4.2. Notwithstanding the provisions of Regulation 14B of the Mandatory Tenders Regulations, 5753-1993, the inclusion of a provider in the digital marketplace will not prevent the Tender Administrator or the Clients from purchasing a similar, identical or equivalent product through a non-public cloud model.~~

~~3.4.3. The terms of this agreement will apply to all customers, which will not be required to sign any additional agreement, except for an on-boarding procedure that may include the customer's approval for the terms of use of the service, as set forth in Section 3.10.~~

3.4.1.1. A similar, identical or parallel service to the service offered in the Digital Marketplace, in a model that is not a public cloud.

3.4.1.2. Other engagement in accordance with the aforesaid in section 3.15.5.

3.4.2. The Tender Administrator and the clients will be entitled to purchase cloud services that are not part of the tender subject in a separate tender or agreement and the Provider will not have any claim against the Tender Administrator if these services are purchased from another provider..

3.5. The engagement period

3.5.1. The engagement will be from the date of enrolling in the digital marketplace until the end of that calendar year (December 31) and will be extended, each year, by another calendar year, unless the Tender Administrator has announced, by December 1, its intent to terminate the engagement. The engagement will end no later than the day of the end of the engagement in the cloud tender, including extensions, if extended.

3.5.2. Subject to the extension of the agreement, during the fifth, tenth, and fifteenth year of the agreement period with the Provider, the Provider may notify the Tender Administrator until June 1 of that same year, of the termination of the agreement, starting from the beginning of the following calendar year.

3.5.3.

Part B – the Services

3.6. Services

3.6.1. Services of the Provider that are set forth in Appendix A will be available for purchase by Clients in the digital marketplace or in any specific digital marketplaces, at the sole discretion of the Tender Administrator.

3.6.2. Appendix A will be updated from time to time according to the services of the Providers that have won the tender in the various categories and changes and additions in the services that were approved by the Tender Administrator for sale in the governmental digital marketplace, according to the provisions of the Tender and Section 3.17 below.

3.6.3. Date of Services deployment in the Israeli region

3.6.3.1. A service listed in **Appendix A** will operate from the Israeli region as an Israeli service by no later than 6 months from the date of winning the Tender, Except in the case of prior written approval having been given by the Tender Administrator approving a different schedule for deploying the service in the Israeli region.

~~3.6.2.1.~~3.6.3.2. If the Israeli region of the Cloud Provider whose cloud platform is to host the proposed service has not yet been established, the service will be provided temporarily until the establishment of the Israeli region, based on an overseas region. In such case, the Provider will transfer the service, including user data, to the Israeli region within 6 months of the day on which the Cloud Provider confirmed that the Israeli region is prepared for ~~operation of marketplace~~

~~services.~~the operation of the service in accordance with the requirements from the Provider, specified in section 3.6.4.

3.6.3.3. The service will be required to comply with all the required standards and the SLA, within 6 months from the date the service began to be provided in the Israeli region at the most.

~~3.6.3.~~3.6.4. The service will be operated in the Israeli region in accordance with the Provider's commonly used configuration for offering the service in other regions overseas where the service is deployed, and in any case the service will be deployed and offered to Clients in more than one zone in the Israeli region, in a manner that will ensure the resiliency and continuity of provision of the service even if one zone fails.

~~3.6.4.~~3.6.5. The services will be ordered from the digital marketplace as stated in the cloud tender and the rules set by the Tender Administrator, which will be updated from time to time.

3.7. Deployment and integration services

3.7.1. The Provider will be allowed to provide deployment services for a service that is available in the digital marketplace, including assistance in operation and deployment of the service correctly and efficiently for the Client and integration with the other systems of the client. To this end, the Provider may use subcontractors.

3.7.2. If the Provider is interested in charging additional payment for such deployment services, in addition to the price of the service in the digital marketplace, it will do so in accordance with the provisions of section 3.15.10 below, after getting ~~the~~ prior written approval ~~of~~by the Tender Administrator. As a general rule, paid integration services will be performed through separate tenders, and the aforesaid approval in this section will be given only in appropriate cases

3.7.3. The Tender Administrator will be allowed to issue directions on the manner of providing such deployment services, including setting a maximum price, a service level agreement and agreed compensation, payment terms and a specific appendix for regulating the provision of these services, and to establish a specific engagement agreement that the subcontractors will sign with the Client as a condition for provision of the services.

3.7.4. The Tender Administrator or the Clients will be allowed to publish a tender or perform any other engagement for receiving integration services for the offered service, in which case the integration services will be provided to the Clients by the selected Provider.

3.8. Documentation

3.8.1. The Provider will provide the Clients, for each service they order, all of the documentation and literature offered by it for Enterprise customers, according to the Provider's public definitions, for that service.

3.8.2. This documentation will include user manuals, directions, settings, printed or electronic updates, "read-me" files, version information and any other update and material related to the service (including all information contained or referred to in the details of use of the service or software), the details of use, operation and maintenance of the service, including any improvement, update or adaptation to those documents, which the Provider publishes or provides to its customers.

3.9. SLA for services

3.9.1. All services provided will be in accordance with the defined SLA that is publicly announced for the overseas region~~ in which the services are consumed,~~ and which applies to Enterprise customers, according to the Provider's public definitions, including the credit /compensation component for non-compliance with this SLA.

3.10. Conditions for using the services

3.10.1. The Client may make any use of the service within the performance of its function and purpose as a public service for the State of Israel and its citizens, subject to statutory provisions applicable to the Client. Besides the statements in this section, there will be no restriction of any kind, including "permitted use" rules for a service being offered in the governmental digital marketplace.

3.10.2. Notwithstanding the foregoing, a Client, or a party on behalf thereof, may not use services for the following purposes:

3.10.2.1. Use for commercial purposes such as resale.

3.10.2.2. Infringement of the Provider’s intellectual property, including reverse engineering.

3.10.3. There will be no ~~restriction~~restrictions on the part of the Provider as to the type of system and information that the Clients may migrate to the service, including vital systems of ~~a~~ high sensitivity level.

3.10.4. There will be no ~~restriction~~restrictions preventing the Clients from transferring content data, including the logic defined by the Client, to another party, including another cloud or service provider.

3.10.5. **~~The terms~~Terms of use for ~~each~~a specified service~~ will be~~**

3.10.5.1. Without deviating from the ~~terms of use set forth~~aforesaid elsewhere in this ~~Agreement. In the absence of an explicit or implicit instruction in the provisions of the Agreement or Tender, the standard, public service~~ agreement~~ of~~, the Provider ~~that is used~~may add terms of for a service, under the following conditions:

3.10.5.1.1. The terms of use are published publicly for customers of the ~~same order~~service in the overseas area.

3.10.5.1.2. The Provider provided the terms of use to the Tender Administrator, in their current form.

3.10.5.2. In any case in which the Provider wants to amend the terms of use of ~~magnitude~~the service, it will be able to do so by providing the Tender Administrator at least 14 days advance notice.

~~3.10.4.1.~~3.10.5.3. In the event that, as ~~the Government~~a result of ~~Israel~~a unique need, the Provider wants a certain term of its terms of use to prevail over the provisions of the agreement (for example - as a result of a new regulation, or a unique feature), the Provider may contact the Tender Administrator with a request for such approval. The Tender Administrator will ~~apply, if any.~~ examine the request and will be entitled to approve, reject or approve the request under conditions, such as for a limited period of time, for specific services or as another relevant condition.

Such approval shall be given in advance in writing and shall be attached to the agreement, as a condition for its entry into force.

3.10.5.4. The status of the terms of use, and the relationship between them and the other terms of the agreement will be in accordance with the provisions in section3.2.3.

~~3.10.5.~~3.10.6. The Provider will not be permitted to apply conditions or additional payment to receiving a service besides the stipulations that appear in the Cloud Provider's marketplace.

~~3.10.6.~~3.10.7. If the Provider intends to stop providing the service from a particular region that Clients are using, it will provide the Tender Administrator and the Clients with at least 180 days' prior notice before terminating the service in that region.

3.10.8. Services purchased by Clients from the Provider, prior to the Provider winning the tender, and which are now available as part of the tender will continue to be provided to the Clients by the Provider. However the terms of these agreements will change and will be in accordance with the terms specified in the tender, except for exceptional cases which received the approval of the Tender Administrator.

3.11. Blocking or restricting use

3.11.1. The Provider will not be able to restrict the Client's use or consumption of any particular service~~ by a Client~~, except as defined for an Enterprise customer, according to the Provider's public settings, subject to its duties in this Agreement, and will not discriminate against Clients in any form or manner.

3.11.2. The Provider will not be able to cancel the provision of the service (service termination) for a certain Client, for any reason, including payment failure~~. Section 3.15 will apply to a case of payment failure.~~ or breach of section 3.10.2. In such cases, and subject to giving a 30-day notice to the Client and the Tender Administrator, the Provider may temporarily freeze or cease the service or the breaching account of the relevant Client and may act in accordance with the provisions of section 3.14.7.

3.11.3. If an order or request has been received from a supra-state entity or tribunal or from a judicial instance, administrative entity, law enforcement or security agencies that are not an organ of the State of Israel (hereinafter jointly and severally: "**foreign entity**") that prohibits or restricts consumption or provision of a service to the Client, and the Provider considers itself compelled to follow that order or request, the Provider will act as set forth below:

3.11.3.1. It will update the Tender Administrator immediately upon learning of the existence of the procedure that is the object of the order or request two workdays at the latest after receiving the order or request, unless it is expressly prohibited from doing so by law.

3.11.3.2. According to the request of the Tender Administrator, and if possible in accordance with the applicable law, it will ask to enroll the Government of Israel as a party to the relevant proceeding.

3.11.3.3. It will ~~take all~~act in accordance with the legal means at its disposal before the judicial instance and the appellate instances to revoke the order or request unless it has received prior written permission from the Tender Administrator not to do so.

3.11.3.4. It will demand that compliance with the provisions of the order or request be in accordance with Mutual Legal Assistance Treaties. If the order or request is not in accordance with the said treaties, the Provider will not comply with the provisions of the order or request, insofar as this is possible under the law of the place from which the service is provided.

3.11.3.5. In addition to the foregoing, if the service is provided from the Israeli region~~,~~ - before fulfilling the provisions of the order or request, the Provider will act in accordance with the relevant Israeli law provisions to enforce the order (such as the Enforcement of Foreign Judgments Law, 5718-1958, the Legal Assistance Between Countries Law, 5758-1998, etc.). In any case, the Provider will not comply with the provisions of the order issued by a foreign entity regarding a service provided to the Government of Israel from the Israeli region when not possible under Israeli law.

3.11.4. If there is an indication that an order or request is expected to be received, as stated above, the Provider will notify the relevant Clients and the Tender Administrator immediately.

3.11.5. Without detracting from any other remedy available to the Tender Administrator, in any case in which intervention from a party extrinsic to the Provider has resulted in a Client being denied the use of a service that is offered to the public by the Provider based on the public cloud, the Provider will take any ~~necessary~~reasonable action under the circumstances to prevent any harm to the Client or to minimize such damage in the given circumstances.

3.12. Essential services and emergencies

3.12.1. In an emergency as determined by the Knesset of Israel, the Government of Israel, the National Emergency Authority, or any party authorized to do so in accordance with any law (hereinafter: “**Emergency**”), or alternatively, in a situation defined by the Tender Administrator as a state of heightened alert, such as: a natural disaster, a national disaster, outbreak of an epidemic, a protracted state of fighting, preparation for war or a military operation (hereinafter: “**State of Alert**”), the Provider will ~~continue~~act with the aim of continuing to provide the services regularly, in accordance with its obligations under this Agreement. For the purposes of this section, an emergency will be a pronouncement made after the date of signing the engagement agreement.

3.12.2. Without detracting from the foregoing, in any case in which a result of an Emergency, a State of Alert or force majeure event the Provider has difficulty in providing a particular service or meeting another obligation that it has under this Agreement, the Provider will contact the Tender Administrator in advance, or in exceptional cases in which this is not possible, immediately and soon after the Provider learns of the difficulty, for the purpose of notifying the Tender Administrator and obtaining its approval, for a limited period of time, for deviating from its obligations under the Tender. In such a case and subject to considerations of fairness and reasonableness, the Tender Administrator will approve the request for a limited period of time, or approve it under conditions, including a condition under which during such period the Clients may purchase the required services from an alternative ~~provider~~Provider.

3.12.3. “Force majeure” for the purposes of this section means: war, invasion by an enemy country, action of an enemy country or battles, insurrection, epidemic, natural disaster, and any other circumstance that the Provider had no control over and could not reasonably anticipate in relation to this engagement with the Government Israel which prevented the Provider from continuing to carry out the works or caused a slowdown in their rate of performance.

Part C – the Digital Marketplace

3.13. Clients

3.13.1. Entities stated below will be considered as Clients for the purposes of the Tender and will purchase services under it in the government digital marketplace or in a specific digital marketplace:

3.13.1.1. Government ministries and auxiliary units – if new government ministries or auxiliary units are established during the engagement period, or government ministries or auxiliary units are split up, the Tender will also apply to the new government ministries or auxiliary units.

3.13.1.2. An outsourcing provider of one of the entities stated above, for the provision of services to the Client, with the approval of the Tender Administrator.

3.13.1.3. Related bodies – during the engagement period, the Tender Administrator will maintain a list of related bodies that are subject to the Mandatory Tenders Law, 5752-1992 (such as government companies, statutory corporations, etc.) that will be considered clients in this Tender. The Tender Administrator will announce the list to the winner and may remove or add related bodies to and from this list.

3.13.2. The decision on whether a particular entity is included in the government digital marketplace or in a specific digital marketplace is at the sole discretion of the Tender Administrator.

3.13.3. The Ministry of Defense and the IDF, when purchasing services from Cloud Providers, will be allowed, by advance notice, to establish, based on this Tender, a specific digital marketplace, which will be managed in accordance with the rules of the Tender.

3.14. Consideration

3.14.1. The consideration to the Provider will be paid by each Client, according to the consumption of services and the rules of the Tender.

3.14.2. The service will be ordered from and the consideration will be paid to the legal entity with which the cloud service agreement was signed (seller of record):

3.14.2.1. AWS EMEA SARL

3.14.2.2. Google LLC

3.14.3. Once the vendor services have been approved for the government digital market on the AWS platform, the vendor must be a registered vendor of AWS EMEA SARL, within 12 months from the date of the announcement of the win.

3.14.4. The payment will be made using the Cloud Providers billing mechanism and it will be made in NIS or in US dollars, according to the conversion rate at the time in which the invoice is issued, and according to the rules of payment that the Tender Administrator will publish.

3.14.5. The date of payment by the Client for a bill that it has confirmed will be no later than 45 days from the time at which the bill was issued to the Client. If the Client refused to pay an invoice or any part thereof for any reason, the Client will explain its decision to do so.

3.14.6. Consideration that is paid to the Provider will be final and no additional amount will be paid to the Provider for the service required of it hereunder. This means that the Provider will not be paid for reimbursement of expenses, payment to subcontractors or payments to third parties, special subscriptions whose price is not included in the service price, training its people (including third parties), security clearance for them or any other expense unless otherwise specifically stated in the tender documents, and with the written approval of the Tender Administrator.

~~3.14.7. Failure to pay consideration~~

3.14.7. Suspension of a service

3.14.7.1. In the event that a Client has not made a payment according to the provisions of this Agreement, or breached a term specified above in the section 3.11.2, the Provider will act as follows:

3.14.7.1.1. The Provider will notify the Tender Administrator of any failure to pay consideration that entails, under its procedures, a freezing or termination of a service or account.

3.14.7.1.2. The Provider is not allowed to delete any information as a result of a failure to pay consideration unless it has received written permission to do so from the Tender Administrator.

3.14.7.1.3. Information that should have been deleted under the Provider’s public policy will not be deleted, and the Tender Administrator will be updated on the exact details of the stored systems, the Client’s details and any other relevant detail that can assist the Tender Administrator in determining the nature and sensitivity of the information. The bill for the costs of storing the information, in the cheapest way, as stated, will be sent for payment by the Tender Administrator.

3.14.7.1.4. Without detracting from the foregoing, if under the Provider’s rules, the process of dealing with a case of failure to pay consideration by Enterprise customers there are arrangements that benefit the customer relative to the procedure above, the beneficial arrangements will apply.

3.15. Rules of conduct in the Governmental digital marketplace

3.15.1. The conduct of the Clients in the digital marketplace ~~will~~shall be ~~operated~~ in accordance with the procurement policy of the Tender ~~Administrator’s policy as~~ Administrator, which will be updated from time to time, the provisions of the applicable law~~,~~ and the government procurement rules, including ~~diversity in cloud procurement and~~ the implementation of the multi-cloud concept.

3.15.2. For non-SaaS service, if the service can be consumed through the services catalog (digital marketplace) of both Cloud Providers in an overseas region, the service must be offered in the digital marketplace of both Cloud Providers.

3.15.3. The Tender Administrator will be allowed to provide instructions to the Clients on the manner of selecting services in the digital marketplace, including competitive proceedings and the like. These instructions will be updated from time to time. The instructions may include attention to the score given for the service evaluation, as set forth in Section 1.3.2 above, which will continue to affect the manner of consumption of the service under the digital marketplace, subject to directions established by the Tender Administrator.

3.15.4. The Tender Administrator may block a service from some or all of the various digital marketplaces, categorically or only for new orders, in cases in which it finds that the price of the service is expensive in its opinion relative to the competition, in the absence of sufficient competition, upon breach of the information or cyber protection rules, or in the case of the Provider not updating or promoting the service or its security as required in the opinion of the Tender Administrator. ~~If possible~~In the aforesaid case, the Tender Administrator will ~~give the Provider notice before blocking a service as set forth~~act in ~~this~~ accordance with the provisions of section 3.15.9, with the required changes, except in an exceptional case where this is not possible due to the need to immediately block the service.

3.15.5. If the Tender Administrator or a Client has conducted a Tender or other central engagement (hereinafter: "**Other Engagement**") for the provision of services for the Clients, the services will be provided by the Providers selected in the Other Engagement rather than through this Tender, and the Tender Administrator may stop or restrict the sale of these services of a certain type or services in the relevant categories in the digital marketplace.

3.15.6. For services provided on the public cloud platform of the Providers winning the cloud tender but having unique characteristics, as determined by the Tender Administrator, the Tender Administrator will be allowed to publish lists of specific requirements and such services will be required to meet these requirements as a condition to continuing the activity in the digital marketplace. In such a case, the provisions of Section 3.15.9 will apply.

3.15.7. The Tender Administrator may perform a central competitive proceeding between services included in the digital or governmental market or services offered to be included in the governmental digital marketplace for the purpose of selecting a central governmental service – a service that will be available for use by all purchasing Clients through the same digital marketplace, in accordance with rules that will be established by the Tender Administrator for a central competitive proceeding ("Central Competitive Proceeding"). It should be clarified that client groups using a particular specific digital marketplace may continue to choose among all the services available in that digital marketplace in accordance with the rules of the Tender.

3.15.8. The Tender Administrator may, for evaluating the information security and cyber protection of the services, demand that the Provider update details and provide additional information in relation to the information provided within its answer to the Tender (not more than twice per calendar year), in accordance with directions that the Tender Administrator will prescribed.

3.15.9. The Tender Administrator will be allowed to update the requirements of the Agreement and the information processing and cyber protection appendices ~~set forth herein.~~specified in this agreement. If the Tender Administrator makes such a change, the following conditions will apply:

3.15.9.1. The changes will only apply to orders that will be sent after those changes take effect.

3.15.9.2. The Tender Administrator will publish the expected changes or will send them to the Provider at least 30 calendar days before they take effect.

3.15.9.3. The Provider will be allowed to send its response to the changes to the Tender Administrator within 21 calendar days.

3.15.9.4. Providers that choose not to implement the required changes may continue to deliver the orders that have been placed until the changes take effect but will not be able to receive new orders or expand their activity under existing orders, except with prior written approval from the Tender Administrator. If at a later stage, the Provider will implement the required changes, the Tender Administrator may cancel the restrictions determined therefor, in whole or in part, in accordance with the sole discretion thereof.

3.15.10. **Private Offer**

3.15.10.1. As part of the sale of services in the digital marketplace, the Provider may submit a private offer in the following cases **only**:

3.15.10.1.1. For a service offered as part of the tender, and when the Provider intends to offer a higher discount percentage than the one offered as part of the tender.

3.15.10.1.2. For deployment and integration services accompanying the service provided as part of the tender, subject to the rules specified in section 3.7 above.

3.15.10.2. A private offer that includes an additional discount for the service in accordance with section 3.15.10.1.1 must be submitted separately from a private offer for deployment and integration services in accordance with section 3.15.10.1.2, such that in the relevant case the Provider will submit two private offers, one with an additional discount for the service and the second with an offer for the deployment and integration services.

3.15.10.3. The Tender Administrator may publish additional rules for submitting a private offer as part of the tender.

3.16. The Tender Administrator’s cyber protection policy

3.16.1. Based on the services and risks involved in using the cloud infrastructures, the Tender Administrator will set a security policy for working in the cloud. This policy will be updated from time to time as the situation dictates. If possible, the Tender Administrator will share with the Providers the relevant parts of this policy, prior to it becoming effective.

3.16.2. The security policy will constitute the manner in which the Agreement is implemented by the Clients and the type of services purchased by them. As such, the Tender Administrator will be allowed to classify services according to their matching the information security and cyber protection level required by the Tender Administrator and Clients and to establish rules for purchasing according to the said classification. In such a case, the Tender Administrator will inform the Provider of the classification of the services it is offering and will inform Clients of the procurement rules in relation to the various services.

3.16.3. The Tender Administrator's cyber policy can take into account procurement diversity involving different providers, including maximizing benefits of implementation in a multi-cloud configuration and cases where there is a preference for consuming services from an overseas region or from another region (other than the Israeli region or overseas region).

3.17. Mechanism for adding or changing services

3.17.1. ~~If~~Without derogating from the Provider's obligations under this agreement, and at most once a year, and if the Provider has made a change in an offered service in a manner that affects its Tender bid (in this respect, a situation in which due to the change it is necessary to update the answer to Appendices 3 or 4 will be considered as affecting a Tender bid), it will announce this to the Tender Administrator and submit the updated appendices. The Tender Administrator may demand that the Provider receive all information and relevant details about the change as a condition to the service continuing to be available in the digital marketplace.

3.17.2. If the Provider is interested in adding another service to the digital marketplace in categories which have already been opened for submission, besides the services offered by it under the Tender, the service will be added in accordance with the following conditions:

3.17.2.1. If the answer to Appendices 3 or 4, as submitted for the service that already exists in the digital marketplace, corresponds with the properties of the new service for the tender, it will contact the Tender Administrator in writing and declare this to it.

3.17.2.2. If the answer to Appendices 3 or 4, as submitted for the service that already exists in the digital marketplace, does not correspond with the properties of the new service for the tender, it will contact the Tender Administrator in writing, resubmitting these appendices for the new service in the process.

3.17.2.3. In both these cases, the Tender Administrator may approve the addition of the service to the digital marketplace, perform a detailed check of the service being offered or demand that the Provider submit the service within a future submission deadline of the Tender.

3.18. Specific digital marketplace

3.18.1. The Tender Administrator will be allowed to establish specific digital marketplaces for a Client or a group of Clients, based on the needs, the information security and cyber protection requirements of those Clients.

3.18.2. The Tender Administrator and the relevant Clients will be allowed to establish specific rules of conduct under these digital marketplaces.

3.19. Changes in the requirements of the Provider given the scope of the engagement

3.19.1. If the scope of orders of a service or group of services provided by the same ~~provider~~Provider exceeds **1 million U.S. dollars in a calendar year**, the Tender Administrator will be allowed to demand for the service / services specific adjustments, such as: increasing the discount rate, updating the information processing and cyber protection requirements, change in work processes and support for users, appointment of an engagement manager who will be the contact person for the Tender Administrator's representative for any matter related to managing the engagement, appointing a representative for finances and billing inquiries and an information and cyber protection officer, according to the requirements that the Tender Administrator will set.

3.19.2. If the sum of orders from a service or group of services provided by the same ~~provider~~Provider exceeds **US$ 5 million in a calendar year**, or if the Tender Administrator chooses the service as a ~~central governmental~~**Government wide service**, the Tender Administrator will be ~~allowed~~entitled, within the timetable to ~~demand~~be determined, subject to the terms of section 3.19.4, to require that the Provider act as follows:

3.19.2.1. Provide the services under this Tender, insofar as it is not doing so, through a corporation in Israel established in accordance with Israeli law, which is registered in the relevant registry in the State of Israel (hereinafter: the “**Israeli Operator**”), with the Provider having 100% ownership and control of the Israeli Operator.

3.19.2.2. **Providing a performance guarantee:**

3.19.2.2.1. To secure meeting of the Provider’s obligations under this Tender, it is to provide an autonomous, ~~unlimited~~unconditional performance guarantee, linked to the consumer price index (the base index being the index known on the day of notifying the Provider of the requirement to provide a guarantee), to the order of the Tender Administrator, in ~~a form that will be established by the Tender Administrator, to~~accordance with the wording stipulated in the Takam Document (Government regulation paper) 7.3.3 – Guarantees (hereinafter: "**Guarantees regulation**"), in a volume of not more than 5% of the volume of actual consumption from the Provider by all Clients in the previous calendar year.

3.19.2.2.2. **The guarantee will be from one of the following entities:**

3.19.2.2.2.1. A bank guarantee from a bank in Israel, which is a banking corporation that has received a bank license pursuant to Section 4(A) (1)(A) of the Banking Law (Licensing), 5741-1981. Alternatively, a guarantee can be submitted from an overseas bank that meets the requirements stated in

~~of Finances and Housekeeping Regulations 7.3.3~~ the Guarantees regulation;

3.19.2.2.2.2. A guarantee from an insurance company in Israel or overseas in accordance with the procedures and criteria set forth in the ~~Finances and Housekeeping Regulations 7.3.3~~ Guarantees regulation.

3.19.2.2.3. For the removal of doubt, the bidder must stay up to date on the directives of the said instruction, before submitting the required guarantee.

3.19.2.2.4. The guarantee will be valid for up to 90 days after the end of the engagement period. If the Tender Administrator exercises the option to extend the engagement period or announces a transition period, the Provider will correspondingly extend the validity of the guarantee by 90 days after the end of the relevant period. Following the expiration date of the validity of the Guarantee, the Tender Administrator will return the Guarantee to the Provider.

3.19.2.2.5. The Tender Administrator is allowed to demand that the guarantee be extended for another three months, in addition to the foregoing, in the event that this will be necessary in order to ensure meeting of the Provider's obligations.

3.19.2.2.6. If the Provider does not extend the validity of the guarantee in accordance with the provisions of the Agreement, the Tender Administrator will be allowed to ~~invoke~~forfeit the guarantee in part or in full, at its sole discretion.

3.19.2.2.7. During the engagement period, the Tender Administrator is allowed, at its sole discretion and at the most once a year, to increase the amount of the performance guarantee in relation to the scope of the engagement, and in accordance with the Tender Administrator's risk management. In any case, the guarantee rate will not exceed 10% of the annual engagement volume of all Clients from the Provider, in the previous calendar year.

3.19.2.2.8. If the guarantee has been ~~invoked~~forfeited in part or in full during the engagement period, the Provider will be required to renew the guarantee, and provide a guarantee to the amount set forth above, as a condition for continuing the engagement.

~~3.19.2.2.9. After the expiration of the guarantee, if it has not been invoked, the Tender Administrator will return the guarantee to the Provider.~~

3.19.2.3. Appointment of representatives on behalf of the Provider in the State of Israel, including the engagement manager on behalf of the Provider and an information and cyber protection officer. The Tender Administrator may demand from the Provider that these representatives be eligible for Level 2 Israeli security clearance.

3.19.2.4. ~~Demanding~~Demand the expansion of the SOC activity hours, as set forth in Section 2.11.19.1 to 7 days a week, 24 hours a day and running of tools for continuous attack surface management as set forth in Section 2.11.19.5.

3.19.2.5. ~~Demanding~~Require an increase in the discount rate, ~~updating~~update the information processing and cyber protection requirements, ~~changing~~change of work processes and support of users.

3.19.3. When ~~demanding~~requiring such changes, the rules set forth in Section 3.15.9 above will apply to all services of the Provider.

3.19.4. ~~The~~Without derogating from the foregoing, the Provider will be given a 6-month grace period for complying with the requirements set forth above.

Part D – general conditions

3.20. Absence of conflict of interest

3.20.1. The Provider undertakes to make every reasonable effort to ensure that the execution of the Agreement does not form any conflict of interest, whether direct or indirect, between it and the Tender Administrator or the Clients.

3.20.2. In the event that there is a concern that the Provider, any employee or another party acting on its behalf may be, directly or indirectly, in a situation of conflict of interest in relation to the provision of services to Clients, the Provider will notify the Client of this without delay and will act immediately to remove the said conflict of interest. In addition, in such a case, the Client will inform the Provider of additional or special measures required of it for the purpose of removing the conflict of interest, which the Provider will carry out as required and as soon as possible.

3.21. Confidentiality of the engagement

3.21.1. The Provider warrants that it and its representative will keep the information that they have received during the performance of their obligations under the Agreement and the Tender in complete confidentiality, during and after the engagement period, and will not use it except for performing their obligations under the Tender and Agreement. Notwithstanding the foregoing, the Provider is entitled to contact the Client or the Tender Administrator in order to allow the disclosure of certain information to any party. The Client or the Tender Administrator will discuss the request and be entitled to accept it, in accordance with their sole discretion, as long as there is no concern that the disclosure of the information will harm the interests of the Clients.

3.21.2. The Provider will not be permitted to announce to any third party which of the services, tools and resources the Clients are using, and what adjustments and uses they are making with these tools, for any reason, including for marketing purposes, without obtaining the advance written permission of the Tender Administrator.

3.21.3. If security clearance classification is required for the purpose of transferring information in relation to the engagement to the Provider, the Provider will provide representatives on its behalf with the required clearance and will ensure that such information is kept only by the holders of the appropriate clearance. If the Provider does not provide representatives with the said clearance, such information will not be transferred to the Provider and the Tender Administrator may restrict the use of the Provider's services accordingly.

3.21.4. The Provider's commitment to maintain the confidentiality of the engagement details will be valid for 7 years beginning on the date of termination of the engagement, unless written permission has been obtained from the Tender Administrator to shorten this period. The statements in this section will not derogate from any duty of secrecy or confidentiality applying to certain information pursuant to relevant statutory provisions.

3.21.5. Without derogating from the foregoing, the Provider is responsible for verifying and ensuring using all means at its disposal that officials working for the Provider and its subcontractors that in the course of their work are exposed to Clients' information (including within the provision of support services, expert services, security incident assistance services, etc.) will keep information disclosed to them completely confidential and will not disclose any information to which they have been exposed to any party.

3.21.6. Revealing or disclosing information as stated in this section, whether by act or omission, other than in accordance with the express prior written consent of the Tender Administrator, constitutes a breach of the Provider's duty of confidentiality, and may constitute a criminal offense under Israeli law, and in particular Section 118 of the Penal Law 5737- 1977, as well as under any other relevant legislation, according to the type of information that will be disclosed (for example: private information, information that is subject to confidentiality under Israeli law, etc~~.)~~.).

3.21.7. Subject to the provisions of the law, the Tender Administrator undertakes to keep the information of the Provider which was received thereby during the agreement in strict confidence. Without detracting from the aforesaid, the parties agree that for the purpose of properly managing the agreement, the Tender Administrator shall be entitled to disclose information regarding the agreement to the Clients or other relevant parties, to the extent and in the required format, including details of the agreement, details of the pricing and any additional relevant details.

3.22. Intellectual property and copyright

3.22.1. To the best of the Provider's knowledge, it owns the rights required in order to provide of the services and their use by the Clients (hereinafter: the "**Intellectual Property**

Rights”). If the Provider does not own the full Intellectual Property Rights, it declares that the owners of the Intellectual Property Rights have given it all the approvals, use authorizations and licenses required under any law for provision of the services and their use by the Clients, in accordance with the terms ~~hereof.~~of this agreement.

3.22.2. The Provider grants the Clients a nonexclusive license to use the services offered by the Provider, as part of the consideration to be paid to the Provider and without any additional consideration. The Provider will not oblige the Clients to purchase licenses for the use of the services and will not subject the use of a service to obtaining a license or purchasing another service, beyond the stipulations set forth in the services catalog (marketplace). It should be clarified that if subscriptions in excess of those provided by the Provider need to be purchased (such as in the case of bring your own license type services or machine images), the Client is allowed to demand the subscription, in any way that it chooses, and not necessarily through this Tender, for which matter the Provider will have no argument.

3.22.3. ~~To the best of~~Without derogating from the Provider’s ~~knowledge, the provision~~ownership of the tools and services ~~and~~ offered in the digital marketplace, any product developed by the Clients or for the ~~Clients’ use of the~~ Clients (including services, systems, applications, products, etc., including intermediate versions), by themselves or through their subcontractor, on top of the Provider’s service or using tools and services of the Provider, will be fully and exclusively owned by the Client and the Provider will not ~~infringe on the~~ have any proprietary thereto. This is true regarding both the financial right and the moral right.

3.22.4. **Intellectual ~~Property Rights~~property infringement**

3.22.4.1. If it has been determined in a final court decision of the competent court that the service offered by the Provider in the Government Digital Marketplace infringes the intellectual property rights of any third party ~~under any law.~~, the Provider will act in accordance with the following:

~~3.22.2.1.1.~~3.22.4.1.1. The Provider will ~~notify~~inform the Tender Administrator ~~in any case in that a legal proceeding alleges that the Clients’ use of the services~~

~~infringes on the Intellectual Property Rights~~and the Clients as soon as possible of ~~any third party~~this occurrence.

~~3.22.2.1.2.~~3.22.4.1.2. ~~If the Provider has learned that the use made by the Clients of the services infringes on the Intellectual Property Rights of any third party, contrary to the provisions of any law, the~~The Provider will make every reasonable effort to make available to the Clients, without additional cost, component or service, whose use does not cause infringement of intellectual property rights, the properties of the substitute component or service not falling short of those of the infringing component or service. The Provider will inform Clients of the reason for substituting the service or component. ~~In any case, the Provider will cease to provide the service that infringes the Intellectual Property Rights of any third party and will credit the Client for any excess amount that it has had to pay for the conduct of the Provider.~~

~~3.22.3. If as a result of an argument that a service that the Clients have purchased from the Provider infringes on a third party's Intellectual Property Right (hereinafter: "**Infringement Argument**"), the Client has sustained damage, the Provider will indemnify the Client for that damage. In this regard, expenses imposed on the Client following a peremptory judgment, proceeding expenses or attorney fees that the Client has been demanded to pay in relation to an Infringement Argument will be considered as damage for this purpose, among other things. In such a case, the limitation of liability set forth in Section 3.26.5 will not apply in such a case.~~

3.22.4.1.3. ~~Accordingly, a Client will notify the Provider of any claim filed against it in relation to an Infringement Argument.~~ The Provider will stop providing the infringing service.

3.22.4.1.4. If any damage is caused to the Client, the Client will be indemnified subject to the provisions of section 3.22.6.

3.22.5. **Infringement claim**

3.22.5.1. If it is claimed in a legal procedure that the use of the services by the Clients infringes the intellectual property rights of any third party (hereinafter: "**Claim of Infringement**"), the parties shall act in accordance with the following:

3.22.5.1.1. If the Client or the Tender Administrator are not a party to the proceedings, the Provider will inform the Tender Administrator and the Clients parties of such as soon as possible.

3.22.5.1.2. If the Provider is not a party to ~~a claim~~the proceedings, the Client will act to ~~enroll it~~add the Provider as soon as possible as a party to the ~~proceeding~~proceedings, in order to enable ~~it to defend himself. In such a case, the Tender Administrator may require~~ the Provider to ~~take the place of~~provide a defense. In the aforesaid case, the Tender Administrator is entitled to request that the Provider will replace the Client for the purpose of conducting the ~~proceeding.~~ procedure.

3.22.5.1.3. In the event ~~of~~that the Client ~~choosing~~chooses to represent itself~~, it~~ in the aforesaid proceeding, the Client will refrain from admitting the ~~claim arguments~~claims of the lawsuit, without the ~~Provider's~~ prior written consent~~. In any case, this will not prevent the indemnification of the~~ of the Provider.

~~3.22.3.1.1.~~3.22.5.1.4. If any damage is caused to the Client, the Client~~, as set forth in Section~~ will be indemnified subject to the provisions of section3.22.6.

3.22.6. **Indemnity for intellectual property infringement**

~~3.22.3.2.~~3.22.6.1. Without derogating from the foregoing, the Provider will indemnify the Client, immediately upon its first demand, for any damage, loss, cost, payment or expense, of any kind and type, sustained by to the Client, according to a ~~peremptory judgment~~final court decision of a competent judicial instance, whose execution has not been delayed, in ~~relation to~~connection with the ~~Infringement Argument. The said~~infringement of intellectual property by the Provider. In this regard, damage will be considered, among other things, as expenses imposed on the Client as a result of a final court decision, costs of proceedings or attorney's fees that were imposed on the Client in connection with the claim of infringement.

In such a case, the limitation of liability specified in section 3.26.5 will not apply. Notwithstanding the foregoing in this section, the aforesaid duty of indemnification of the Provider will not apply in ~~the following~~ cases in which the judgement determined that:

~~3.22.3.2.1.~~3.22.6.1.1. 3.22.6.1.1 The Infringement ~~Argument~~ (if ~~any~~ it was determined that there is such) stems from a use made by the Client in contravention of the provisions of this Agreement, when the action that was a breach of the Agreement is what actually caused the infringement of the Intellectual Property Rights.

~~3.22.3.2.2.~~3.22.6.1.2. ~~If it is determined by a judicial instance in a peremptory judgment whose execution has not been delayed that the infringement of Intellectual Property Rights~~3.22.6.1.2 The infringement is not due to the Client's use of the Client's services per se, but that the infringement is a combination of ~~the~~that same service with a product or service provided by a party extrinsic to this agreement, or if developed by the Client itself.

~~3.22.4. Any product that has been developed by or for the Clients (including services, systems, applications, products, etc., including intermediate versions), by themselves or through a subcontractor, on the service of the Provider, or using the Provider's tools and services, will be fully and exclusively owned by the Clients, and the Provider will have no proprietary claim thereto. This applies to economic rights and moral rights alike.~~

3.23. Relations between the parties

It is hereby declared and agreed between the parties that:

3.23.1. This Agreement does not form between the parties to the Agreement any employer-employee relations. The Tender Administrator and the Clients are not the employer of the Provider, any of its employees or the employees of its subcontractors.

3.23.2. The Provider will be solely responsible for any payment, indemnification for damages, compensation or any other payment due therefrom under any law to the persons employed by it, or to any other person.

3.23.3. The Tender Administrator and the Clients will not pay any payment for national insurance or other social benefits for persons employed by the Provider or its subcontractors.

3.23.4. If notwithstanding the foregoing, a competent judicial or administrative instance has ruled in a ~~peremptory judgment~~final court decision whose execution has not been delayed that the Client bears direct responsibility towards the Provider, its employees or subcontractors, arising from recognition of employer-employee relations between the Client and the Provider or any agent thereof, the Provider will indemnify the Client for any it is charged that exceeds the consideration owed to it hereunder. This includes the Provider bearing court expenses and attorney fees borne by the Client.

3.23.5. In the event of a claim being filed as set forth in this section against the Tender Administrator or the Client, the Client will notify the Provider of the existence of the claim as soon as possible after receiving it and will allow the Provider to defend itself. If the Tender Administrator or Client intends to compromise with the plaintiff, a notice of this will be given to the Provider in advance.

3.24. Subcontractors

3.24.1. The Provider will be allowed to employ subcontractors to provide the services subject to the statements in the tender documents. In the aforesaid case, the subcontractors will act in accordance with all the relevant obligations applicable to the Provider.

3.24.2. The overall responsibility for provision of the services and compliance with all of the conditions of the Tender will be assumed by the Provider, and all engagements of parties of the Client in relation to works will be done with the Provider only.

3.24.3. In any case of the ~~provider~~Provider employing a specific subcontractor for providing services to Clients according to the provisions of the Tender and for this purpose only, the Tender Administrator will be allowed to demand that the Provider change this subcontractor if it believes that it is not performing its duties as required. ~~Before~~30 days prior to demanding the replacement of the subcontractor, the Tender Administrator will forward ~~a~~an explanatory notice of intent to demand such replacement.

3.25. Payment rules

3.25.1. The payment rules set forth below are subject to the instructions of the Accountant General in the Ministry of Finance as published from time to time.

3.25.2. In order to receive payment, the Provider will submit each month, through the Cloud Providers' billing and payments system, for each Client, a bill detailing the payments due to it in accordance with the Agreement and the Tender and the rules of the digital marketplace (hereinafter: "**Bill**"). A Bill is not to be submitted to Clients in any other way.

3.25.3. The Tender Administrator will be allowed to instruct the ~~providers~~Providers in relation to information that is to be specified in the Bill.

3.25.4. If the invoice is subject to statutory VAT, the Bill must include, among other things, the amount to be paid before value added tax (hereinafter: "**VAT**"), and the total amount to be paid including VAT.

3.25.5. In the event that there are changes in taxes or duties applying to the Provider in relation to the price of the services or goods, and if these changes are not in the VAT rate, these changes will not affect the amount of consideration, except according and subject to receiving prior written approval from the Client, at its sole discretion.

3.25.6. The date of payment for a Bill approved by the Client will be no later than 45 days from the date that Bill was issued to the Client.

3.26. Liability for damage

3.26.1. The Provider will be liable for any damage or loss of any kind incurred by the Client, its employees or any agent on its behalf as well as any entity, person or any third parties, due to an act or omission of the Provider, its employees, agents, subcontractors or anyone acting on its behalf or in its place, as part of the implementation of this Agreement~~.~~, up to the liability limit specified in section 3.26.5.

3.26.2. The Client, its agents and employees will not be held liable will not bear any payment, expense, loss or damage, owing to any loss or damage of any kind incurred by the

Provider, its agents or employees. The foregoing will not apply to damage caused by malice or gross negligence for which the responsibility is assumed the Client by law.

3.26.3. The conclusion of this Agreement will not derogate from the Provider’s liability for damage for which the cause of action arises from this Agreement or from the provision of the Services hereunder or that is related thereto.

3.26.4. The Provider undertakes to pay and indemnify the Client in full, insofar as the Client is compelled by a ~~peremptory judgment~~final court decision of a competent judicial instance, whose execution has not been delayed, to pay any amount for a charge that is payable hereunder by the Provider, whether arising from a claim by an employee of the Provider or any agent thereof (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 specified in section 3.26.5.

3.26.5. ~~The~~Unless specifically written otherwise as part of this agreement, the limit of the Provider’s liability for compensation or indemnification of the Client for any damage event will not exceed the amount of the damage caused or the indemnification required, up to twice the volume of the actual consumption of services from the Provider by all Clients in the 12 months preceding the damage event, whichever the lower, plus all expenses of the Client, including legal expenses and attorney fees that it has had in relation to a claim for the foregoing, plus linkage differentials and statutory interest. ~~The said amounts will be paid to the Client immediately upon submission of its written demand detailing the expenses incurred by it as aforesaid.~~ Such limitation of liability will not apply to damage caused by a malicious act or omission by the Provider, its employees or subcontractors or anyone acting on its behalf.

3.26.6. The Client will notify the Provider of any claim or demand under this section as soon as possible after receiving it and will allow the Provider to defend itself against it. In such a case, the Client will not agree to arguments raised or made against the Provider, for which the liability under this Agreement is assumed by the Provider, without the prior written consent of the Provider, and will notify the Provider in advance of its intention to compromise with the plaintiff.

3.27. Insurance

3.27.1. The Provider undertakes to arrange and maintain appropriate insurances for the services it provides ~~for the State of Israel, Government ministries, auxiliary units and related bodies~~to the Clients, as is customary in its field of activity (for example: professional liability insurance combined professional / product liability insurance, cyber insurance or other insurance, as the case may be) within reasonable liability limits depending on the nature and scope of the services provided by it, and shall cover the services provided through this contract. If the Provider employs subcontractors, it must demand that they execute insurances for covering their direct liability, as required in this section, or to make sure that its insurances include coverage for their activity and direct responsibility.

~~3.27.2. The Provider warrants that the limits of liability and the terms of coverage in the insurance it will possess are required to be in accordance with the scope of the engagement and the extent of the risks that may arise from the engagement. The Provider must examine and evaluate its potential exposure to liabilities and increase the limits of liability as necessary.~~

~~3.27.3.~~3.27.2. The Provider undertakes to comply with the terms of the insurance policies made by it, to pay the insurance premiums in full and on time, to verify and ensure that its insurance will be renewed from time to time as necessary, and will be valid throughout the service provision period, as long as it has responsibility. For the removal of doubt, it is clarified that the deductible payment in any insurance case will be borne by the Provider only.

~~3.27.4. If subcontractors (including sub-processors) are employed by the Provider, it must make sure that its insurances include coverage of its liability for them, and demand that they acquire insurances to cover their liability, as required by this section, or ensure that its insurance covers their activity and liability.~~

~~3.27.5.~~3.27.3. The Provider will ensure that in all its insurances covering ~~to~~ the services that are the ~~object~~subject of the ~~engagement~~agreement, the ~~Client~~Clients will be added as an additional ~~insured~~insuree, subject to the ~~extension~~expansion of the indemnity ~~towards the Client~~, as is ~~commonly practiced for~~customary in that type of insurance.

~~3.27.6.~~3.27.4. If the Provider reaches an annual purchase sum of US$ 1 million from the Clients according to the Tender, it will ensure that all its insurances applying to the services that are the object of the engagement will include a clause of waiver of right of subrogation towards the Client and its ~~agents~~employees (such a waiver will not apply to malicious damage). In addition, the Provider will make sure that all of its relevant insurances ~~as set forth in Section 3.27.1 will have~~include a cross-liability clause and ~~will constitute a policy taking precedence over~~ initial clauses in any other policy ~~will apply to an~~of the Clients. In addition, the insurance ~~event~~will include a clause whereby the law, jurisdiction and territorial borders also include the State of Israel.

~~3.27.7.~~3.27.5. The Tender Administrator reserves the right to obtain from the Provider a certificate of maintaining insurance ~~or copies of~~ policies,~~ from time to time and~~ upon demand.

3.28. Assignment of rights or obligations by agreement

~~3.28.1.~~ The Provider is strictly prohibited from assigning or endorsing any right or obligation under this Agreement or the performance of the actions stated herein, in part or in full, to other parties, without the prior written approval of the Tender Administrator, at its sole discretion. ~~An exception is assignment of rights between companies that are fully owned by the global corporation directly or in a chain of companies, which does not require the prior consent of the Tender Administrator, provided that such an assignment does not contradict the provisions of the Agreement or impact the Clients, or the service provided under this Agreement.~~

~~3.28.2.~~3.28.1. Assignment of rights or obligations under this section will be made subject to the signing of a "back-to-back" agreement between the assigner and the assignee. The said agreement will be sent to the Tender Administrator before and as a condition to the assignment of rights or obligations taking effect.

3.28.2. Notwithstanding the provisions of section 1.1.1, the assignment of rights between companies that are fully owned by the Provider or the parent company of the Provider directly or under a chain of companies does not require the prior consent of the Tender

Administrator, provided that such an assignment does not contradict the provisions of the Agreement or impact the Clients, or the service provided under this Agreement.

3.29. Termination of the engagement

3.29.1. If part or all of the engagement with the Provider has been terminated or canceled, for any reason, the following rules will apply:

3.29.1.1. The Clients and the Tender Administrator may engage in an agreement with another provider on the subject of the Tender.

3.29.1.1.1. The said termination of the engagement will not cancel orders already received by the Provider.

3.29.1.1.2. Services that have already been purchased in accordance with the provisions of the Agreement will continue to be run according to the terms prescribed herein~~.~~, in accordance with the terms of the agreement.

3.29.1.1.3. Without derogating from any other provision herein, the Provider will cooperate with the Client in the transfer of content data and products of the Clients that are in its services to the Client, and in any case will not restrict or prevent the transfer of information or configurations from its systems, in any form or manner, except in the case of damage to the intellectual property of the Provider.

3.29.1.1.4. After completing the transfer of the information to the Client, the Provider will delete all content data or processing data of the Client that are in its systems, in such a manner as to prevent restoration.

3.29.2. Without detracting from the entirety of the provisions of the agreement, the Tender Administrator may terminate the engagement with the Provider, ~~by 30 days' prior notice,~~ ~~in~~subject to the provisions of section 3.30.2, upon the occurrence of any of the following cases:

3.29.2.1. If a pre-liquidator, temporary liquidator or permanent liquidator is appointed for the Provider;

3.29.2.2. If a temporary or permanent receiver for the business affairs or property of the Provider is appointed;

3.29.2.3. If the Provider has been issued an order to instigate proceedings under the Insolvency and Economic Rehabilitation Law, 5768-2018, or an ~~equivalent~~ order with a similar significance in another country;

3.29.2.4. If the Provider has become bankrupt, or has withdrawn from the execution of the Agreement for any other reason;

3.29.2.5. The Provider must immediately notify the Tender Administrator of the occurrence of one of the cases stated in this section.

3.29.3. In any case in which the engagement with the Provider has been terminated or canceled, the Clients will pay the Provider the consideration for the services that have been purchased and actually provided by the Provider in accordance with the provisions of the Agreement, until the date of termination of the engagement.

3.30. Breach of the Agreement

3.30.1. Fundamental breach of the Agreement –

3.30.1.1. **The following will be considered as a fundamental breach of the Agreement (hereinafter: "fundamental breach"):**

3.30.1.1.1. A critical security incident at the Provider's premises, with a direct impact on the Clients or on essential services provided by them.

3.30.1.1.2. Change of prices relative to those set forth in the Tender and in the bid submitted by the Provider.

3.30.1.1.3. Behavior in bad faith, trickery or dishonesty by the Provider, including providing misleading or inaccurate information.

3.30.1.1.4. If the Provider has withdrawn from performing the Agreement.

3.30.1.2. **If the Provider of has committed a fundamental breach of the Agreement, the Tender Administrator will act as follows:**

3.30.1.2.1. The Tender Administrator will allow the Provider to rectify the defect, within 10 working days of receiving a written notice from the Tender Administrator, or within a longer time as prescribed by the Tender Administrator depending on the circumstances of the case. In any case in which the breach has not been rectified within the time limit prescribed to that end, the Tender Administrator will be allowed to notify the Provider with 21 days' prior notice of the termination of the engagement.

3.30.1.2.2. If, as a result of the fundamental breach, the Clients or the Tender Administrator are likely to sustain damage immediately, the Tender Administrator may, at its sole discretion, immediately terminate the engagement with the Provider or any part thereof without prior notice, without derogating from the Tender Administrator's right to ~~invoke~~forfeiture the performance guarantee, and any other relief or Compensation as stated in the Tender, in the Agreement or under any statute.

3.30.2. **Non-fundamental breach of Agreement –**

3.30.2.1. **Cancellation of the Agreement due to a breach or expected breach~~—~~:**

3.30.2.1.1. Without derogating from the foregoing, in any case of failure of the Provider to meet its obligations under the Tender and the Agreement, for any reason, the Provider will be allowed to rectify the defect within 25 working days of receiving written notice from the Tender Administrator, or within a longer period that the Tender Administrator will prescribed given the circumstances at hand.

3.30.2.1.2. In any case in which the breach has not been rectified within the time prescribed for doing so, the Tender Administrator will be allowed to notify the Provider by 180 days' advanced notice of the termination of the engagement owing to breach of the Agreement.

3.30.2.1.3. If the Provider has learned of a likely possibility that it will not be able to meet some or all of its obligations for any reason (in this section – “expected breach”), or that it will not be able to meet the deadlines and conditions of the service, it will immediately notify the Tender Administrator of this orally and by email.

3.30.2.1.4. In any case of an expected breach of the Agreement, the Provider will bring its plan to meet its obligations hereunder in the best possible way under the given circumstances to the Tender Administrator for approval. If the Provider acts in the manner approved by the Tender Administrator, the forms of relief set forth in this Agreement for breach hereof will not be applied against it.

3.30.2.2. Hearing before cancellation of Agreement owing to breach

3.30.2.2.1. Without derogating from the foregoing, in any case in which the Tender Administrator intends to order the cancellation of the Agreement owing to any of the causes for cancellation set forth above, except for immediate cancellation as a result of a fundamental breach or concern of immediate damage, the Tender Administrator will subject the Provider to a hearing, which will be held in writing or orally, according to the Tender Administrator’s decision, in which the Provider may state its arguments.

3.31. Remedies for breach of agreement

3.31.1. In any case of breach of agreement, each of the following remedies will be available to the Tender Administrator, jointly and severally:

3.31.2. ~~Offset~~Deduction and lien –

3.31.2.1. The Tender Administrator and the Clients will have the right to ~~offset~~deduct from amounts they owe to the Provider under the Agreement against any debt that the Provider owes to one of them hereunder, whether fixed or not, including between orders. The Tender Administrator and the Clients will also be allowed to withhold from the Tender Administrator any amount they owe to the Provider, until any debt that the Provider owes any of them is repaid.

3.31.2.2. The Provider will not have any right of ~~offset~~deduct or lien against the Tender Administrator or any Client in respect of any amount that it argues any of them owes it.

3.31.3. **~~Invocation~~forfeiture of performance guarantee –**

3.31.3.1. If the Provider has provided a performance guarantee, the Tender Administrator will have the right, in accordance with the provisions of the Agreement and subject to giving a notice as set forth below, to ~~invoke~~forfeiture the performance guarantee that the Provider has provided.

3.31.3.2. The Provider will be notified in writing 7 calendar days in advance, at least, before the Tender Administrator applies the relief available to it under this section.

3.31.4. **Cumulative remedies**

3.31.4.1. The remedies, including the right of ~~offset~~deduct and ~~invocation~~forfeiture, liquidated damages, and all actions authorized by the Tender Administrator in this Agreement in response to breach of the Agreement by the Provider, are cumulative, and no provision herein will deny the Tender Administrator any right to any relief or remedy hereunder or by statute.

3.31.4.2. If the Tender Administrator waives its rights due to a breach of any provision of this Agreement by the Provider, this will not be construed as a waiver of any other breach of that or another provision.

3.32. Changes to the Agreement

3.32.1. Any change to the Agreement will be made with the consent of the parties and through the signing of an addendum to this Agreement. The addition will specify the changes from the arrangements set forth herein.

3.32.2. This Agreement contains all of the covenants between the parties, and no agreement or arrangement made prior to the signing of this Agreement will be valid.

3.33. Addresses of parties and notices

3.33.1. The address of the Tender Administrator: Government Procurement Administration, 1 Netanel Lorch St., Jerusalem;

3.33.2. The Provider's Address: ____;

3.34. The applicable law and unique place of jurisdiction

3.34.1. The parties agree that the jurisdiction on all issues and matters arising out of or relating to the Agreement or the provision of services that are the object of the Agreement, or in any claim arising out of or relating to the engagement or its conduct will be conferred solely to the competent courts in the Jerusalem District and that Israeli law will apply.

3.35. Undertakings and declarations of the Provider

3.35.1. **The Provider declares and undertakes as follows –**

3.35.1.1. There is no statutory impediment to its engagement in this Agreement.

3.35.1.2. It meets all the relevant statutory requirements for the provision of cloud services to the Government of Israel, in accordance with the Agreement.

3.35.1.3. In any case in which there are changes in the provisions of law applicable to the Provider, in a manner that affects the execution of the Agreement, the Provider will act efficiently and quickly in order to adapt the services to the statutory requirements and will bear the costs involved in these changes.

3.35.1.4. It has the experience, skill, knowledge, tools, inventory and personnel necessary to meet its obligations in accordance with the terms of the Agreement and the Tender.

3.35.1.5. Anyone who takes part in the provision of services on its behalf in the framework of the Tender is qualified and competent for his function.

3.35.1.6. It will deliver everything required of it in accordance with the requirements of the Tender.

3.35.1.7. It will cooperate with the Tender Administrator and the Clients their representatives in all matters relating to the meeting of its obligations hereunder.

4. Appendix C1 – Information Processing for services in software as a service (SaaS) configuration

4.1. Protected information

4.1.1. Without derogating from the Provider's obligation elsewhere, the Provider will be responsible for the safeguarding, protection and integrity of the protected information on its systems, and will not access it, will not allow any other party to access it, will not use or modify it, and will not permit any use or modification, by act or by default, which is not permitted according to the provisions of Israeli law, the provisions of the Agreement and this Appendix.

4.1.2. The Provider will be responsible for ensuring that Clients and users have regular access to the protected information, in accordance with its obligations under this Agreement, and in any case will not deny them access to such information, in a manner that contravenes the provisions of the Agreement or Israeli law.

4.1.3. The Provider understands that the protected information includes information about the work processes of the Government of Israel and information pertains in part to the citizens and residents of the State of Israel. Accordingly, any disclosure, compromising, damage, denial of access or loss of protected information or disclosure of information to a third party may cause the Tender Administrator, Clients, users and third parties heavy damage, and it will be required to safeguard the protected information in accordance with the highest standards existing in the marketplace, and will not transfer it to any third party, in accordance with the provisions of this Appendix.

4.1.4. Protected information will not be kept on public cloud infrastructure that is not one of the Cloud Providers winning the cloud tender.

4.1.5. The Provider's obligations in relation to the Protected Information will apply as long as the information is in its systems, even after the end of the engagement period.

4.1.6. The Provider will allow complete logging and documentation of all access to and use of the various services by the Client and its users.

4.1.7. Keeping of the documentation for a period of at least one year will be possible, meaning that it will be continuously available to the Client and to the Tender Administrator.

4.2. Content data

4.2.1. The Clients will be allowed to produce content data in or through the Provider's systems and to migrate to the Provider's cloud systems any content data as they wish, subject to the provisions of the law, including content data with different levels of sensitivity, including content data of Clients that are subject to various statutory restrictions, for which the Provider will have no argument and will impose no restrictions.

4.2.2. Under the Israeli law applying to the content data of some of the Clients as updated from time to time, there are requirements regarding the protection of the information against defacement, alteration and unauthorized disclosure. Among other things, the statutes that apply to information include, the Regulation of Security in Public Bodies Law, 5758-1998, the Commercial Torts Law, the State Property Law, as well as specific statutes that apply to the activity of the state and government employees in various fields. The statutory obligations towards the Protected Information are imposed on the Clients only, which own the information, and not on the Provider, unless expressly stated otherwise in the tender documents. The Provider's duty is to make every reasonable effort to allow the Clients and the Tender Administrator to discharge the various statutory obligations applicable to them with respect to such Protected Information. Nothing in this section will derogate from any statutory obligation imposed on the Provider.

~~4.2.3.0.1.1.1.1.Within 30 days of the Client's request or within 30 days of the ending of the engagement, for any reason, the SaaS provider will provide the Client with all of the Client's information. If the service allows the Client to retrieve or delete information directly, the Provider will allow the Client to do so 30 days after the end of the engagement while providing reasonable technical assistance by the Provider to retrieve and delete the information and will show the Client documented proof that all information has been retrieved or deleted as required. All information will be retrieved in a standard, up-to-date and non-proprietary format.~~

4.3. Use of Protected Information

4.3.1. The Tender Administrator and the Clients are the sole owners of the Protected Information, and the Provider constitutes a processor of the Protected Information and will not take any action, including saving and storage, processing of information and transfer thereof to any third party except in accordance with applicable statutes in the State of Israel and as set forth below:

4.3.1.1. For content data – with the approval of the Client, according to a digital instruction, for the purpose of correct provision of the purchased services.

4.3.1.2. For processing data – at the minimum level required for the correct provision of the services purchased under the Agreement, including improving the cyber protection of the Provider's systems or the services, for charging for them and discharging the Provider's obligations under the Agreement. It should be emphasized that the use of processing data for the purpose of improving the services of the Provider that is not part of the improvement of those services for, among others, the Clients, is prohibited except in the case of obtaining written permission from the Tender Administrator.

4.3.1.3. For access data – at the minimum level required for the proper delivery of the services purchased under the Agreement, for charging for them and for the meeting of the Provider's obligations under the Agreement.

4.3.2. Without derogating from the foregoing, and for the removal of doubt, the Provider will not sell, rent out or perform any other commercial operation using Protected Information, including the transfer of the information after processing, the transfer or sale thereof as part of other users' information after deleting identifying details, or in any other constellation.

4.3.3. The Provider will not store Protected Information on its systems other than in accordance with the provisions of the Agreement and this Appendix, and according to a digital instruction, and will ensure the purging of such information contained in its systems, according to statutory provisions.

4.3.4. Without derogating from the Provider's obligations, the Provider will take the necessary precautions to ensure that access to Protected Information is granted only to parties that authorized ~~employees of~~by the Provider for whom access to this information is required for the provision of the services to Clients. The Provider must ensure that the disclosure and use of Protected Information to and by authorized parties will be to the minimum extent required for the purpose of providing the service properly, and in accordance with the Provider's obligations. The Provider will instruct the authorized parties on the purposes of the use of the information, and the obligations imposed on them by law and the provisions of hereof as a result of having the information disclosed to them.

4.3.5. Deletion of Protected Information

4.3.5.1. ~~According~~Within 30 days of the Client's request or within 30 days from the termination of the engagement, for any reason, the SaaS Provider will provide the Client with all of the Client's information. If the service allows the Client to retrieve or delete information directly, the Provider will allow the Client to do so within 30 days after the end of the engagement while providing reasonable technical assistance by the Provider to retrieve and delete the information and will show the Client documented proof that all information has been retrieved or deleted as required. All information will be retrieved in a standard, up-to-date and non-proprietary format.

~~4.3.5.1.~~4.3.5.2. Within 30 days following the end of the engagement or according to a digital instruction to delete information or after the end of use of the service and according to the terms of service, the Provider will completely delete all copies of the content data in its systems or service environments in a way that will preclude its restoration, unless otherwise stated in this Agreement.

~~4.3.5.2.~~4.3.5.3. ~~After the customer's use of the Service ends,~~Further to what is detailed above and subject to its statutory obligations, the Provider will delete from its records and databases all processing data and access data necessary for performing the permitted operations set forth in this section.

4.4. Confidentiality

4.4.1. The parties agree that the Protected Information is confidential and may not be used contrary to the provisions of the Agreement or passed on to any other party without prior written permission from the Tender Administrator.

4.4.2. The Provider undertakes to keep secret security tools, including encryption tools such as stamps and encryption keys, which it makes available to the Client, and not to provide any other party tools or technological assistance for decoding the security tools, without prior written permission from the Tender Administrator.

4.4.3. Without derogating from the foregoing, the Provider will be obliged to take all necessary steps for the purpose of maintaining the confidentiality of access data and processing data kept in the Provider's systems in a confidential and secure manner, as part of which the Provider undertakes as follows:

4.4.3.1. That this data will be ~~kept~~protected using state of the ~~most advanced~~art technological means available in the market.

4.4.3.2. That access to this data by the Provider's employees will be made only by authorized persons requiring this access, and only to the minimum extent required.

4.4.4. The Provider will be responsible for its sub-processers that will have access to Protected Information from it for the purpose of providing the services to the Clients, will be bound to confidentiality as set forth in this Appendix, and in any case it will be fully responsible for any breach of this duty by them.

4.5. Privacy

4.5.1. Without derogating from its obligations in the Appendix and the Agreement, the Provider undertakes to act in accordance with the provisions of the Protection of Privacy Law, 5741-1981 (hereinafter: "**Protection of Privacy Law**") and its regulations and any other legislation under Israeli statutes that regulates privacy under the Israeli Law, in order to allow Clients to upload private information that is protected under the relevant legislation (hereinafter~~—~~: "**Private Information**") to the cloud. It should be emphasized in this respect that different Clients have different, diverse types of Protected

Information at different levels of sensitivity, such as, “medical information”, as defined in the Patient’s Rights Law, 5756-1996 personal information, and so on.

4.5.2. The Provider will attach to the terms of use (Service Agreement) an appendix detailing the compliance with the obligations imposed on the Provider under the Protection of Privacy Law and the regulations enacted thereunder (hereinafter: “**Privacy Appendix**”).

4.5.3. The provisions of the Privacy Appendix will comply with at least the Provider’s obligations under this Agreement and this Appendix. The Tender Administrator may require the Provider to make adjustments in the Privacy Appendix, for the purpose of complying with the provisions of the law, the Agreement and this Appendix.

4.5.4. The Provider will update the Privacy Appendix, according to changes in Israeli law in relation to the Private Information that the Clients possess, in a manner that will allow the Clients to keep Private Information in the cloud throughout the engagement period.

4.5.5. For an Israeli service, the Provider will not take any Private Information out of the borders of the State of Israel, except in the case of a digital instruction from the Client or with the prior written permission of the Tender Administrator, under conditions that it will prescribe.

4.5.6. For a non-Israeli service, the Provider will not take any Private Information out a region within the borders of the European Union, and the rules of the General Data Protection Regulation (GDPR) will apply to it.

4.5.7. Without derogating from the Provider’s obligations, the Provider will keep Protected Information under its technical control, such as processing data or access data in accordance with the provisions of the law and in particular under the Protection of Privacy Law and its regulations.

4.6. Criminal prohibition against disclosing Protected Information

4.6.1. Exposure or disclosure of confidential information under this Agreement, whether by act or omission, and which is not in accordance with the express, written consent of the Tender Administrator, constitutes a breach of the Provider’s duty of confidentiality under this Agreement and constitutes a criminal offense under Section 118 of the Penal Law, 5737-1977.

4.6.2. In addition, depending on the type of information that is disclosed, disclosure of Protected Information, whether by act or omission, other than according to the provisions of the Agreement or statutory demands, may constitute a criminal offense under Israeli law, depending on the type of information disclosed (for example: Private Information, information that is privileged under Israeli law, information that could harm the state security of the state, etc.).

4.7. Israeli service

4.7.1. All content data will be kept within the borders of the State of Israel, unless otherwise stated under this Agreement.

4.7.2. The content data contained within the State of Israel will not be taken out of the borders of the State of Israel for any purpose, including processing, storage, backup or for transfer to a third party without a digital instruction from the Client or with the prior written permission of the Tender Administrator, under conditions that it will prescribe.

4.7.3. If the Provider removes Protected Information from the borders of the State of Israel, it will delete the Protected Information immediately, and as long as this is done for the purpose of providing service in accordance a digital instruction, immediately upon completion of the operation, according to the digital instruction, and subject to legal provisions.

4.7.4. In any case, the Provider will not keep information in a State that does not maintain diplomatic relations with the state of Israel.

4.8. Applicable law and jurisdiction for Protected Information

4.8.1. **Without derogating from the statements in Section 3.34 of the Agreement:**

4.8.1.1. The State of Israel has a full, exclusive sovereign interest, and full powers over and ownership of the Protected Information. As such, the law that applies to Protected Information is the law of the State of Israel, and the courts of the State of Israel have exclusive jurisdiction to hear any question or proceeding concerning the said information, without qualifications or exceptions.

4.8.1.2. For any direct conflict between the Provider and the Tender Administrator in relation to the Protected Information, the applicable law will be Israeli law and the jurisdiction to hear any question or proceeding concerning the said information will be conferred exclusively to the courts of the State of Israel, without qualifications or exceptions.

4.8.2. The Provider will immediately announce any changes or updates in the legal situation applying to it that affects the exercising of the duties and rights in relation to the Protected Information under this Agreement. For the removal of doubt, such a change will not exempt the Provider of its obligations in accordance with the provisions of the Agreement.

4.9. Unlawful transfer of information

4.9.1. Notwithstanding the provisions of Section 4.8.1, if the Provider has received a request or order from a foreign entity for receiving, deleting, altering or denying access to Protected Information, and in the opinion of the Provider, the said request or order legally obligates it, whether or not the information is within the State of Israel, the Provider will act as set forth below:

4.9.1.1. It will announce the request or order as soon as possible to the relevant Tender Administrator and Client and will update them on the steps it has taken through to that stage, unless it is expressly prohibited by law from doing so.

4.9.1.2. If there is a confidentiality order applying to the issue of the request for information itself, the Provider will act to remove the order, and to allow for the Tender Administrator to be notified of the existence of the request.

4.9.1.3. It will refuse to consent to the transfer the information, and will make any relevant legal arguments, including one that the information belongs to a sovereign state, and that the information is subject to state immunity.

4.9.1.4. If necessary, it will appeal the decision to a judicial instance or relevant administrative authority until all the possible appellate instances are exhausted, including filing a motion to stay execution until a final decree on the matter.

4.9.1.5. At the request of the Tender Administrator, it will request to enroll the Government of Israel as a party to the relevant proceeding.

4.9.1.6. It will act to reduce the scope of disclosure of the information only to relevant information in the request.

4.9.1.7. It will demand that compliance to the request or order be in accordance with mutual legal assistance treaties, and it will not comply with a request or order unless permitted by law in the territory in which the Protected Information is located.

4.9.2. In addition to the foregoing, if the Provider has received a request or order from a foreign entity for receiving Protected Information located in the State of Israel, and in the opinion of the Provider such an order legally obligates it, in addition to the statements in Section 4.9.1, the Provider will operate as set forth below:

4.9.2.1. The Provider will follow the provisions of Israeli law for enforcing the order (such as under the Enforcement of Foreign Judgments Law, 5718-1958, the Legal Aid between Countries Law, 5758-1998, etc.).

4.9.2.2. In any case, the Provider will not enforce an order issued by an organ of a foreign state on Protected Information of the Government of Israel located in the territories of the State of Israel, when not possible under Israeli law.

4.9.3. Without derogating from the Provider's obligations elsewhere, the provisions of this section will apply to the Provider even if the request from foreign entity was received at a sub-processor or other subcontractor operated by it for the purpose of providing the services under the Agreement and possesses the Protected Information. In such cases, the Provider will take the place of its processor or subcontractor and act in accordance with these obligations.

4.9.4. If the Provider has an indication that a such request or order is expected to be received as set forth in Sections 4.9.1-4.9.2 above, it will notify the Tender Administrator about this immediately, unless it is barred from doing so by law.

4.9.5. **Actions are required in cases of sending of Protected Information**

4.9.5.1. Without derogating from the Provider's statutory responsibility, and without limiting its obligation under this Agreement, in any case in which the Provider has sent Protected Information to a third party that is not permitted to have it according to the Tender Documents, for any reason, including as a result of a request or order from a foreign entity, the Provider will act as follows:

4.9.5.1.1. The Provider will inform the Tender Administrator as soon as possible of any Protected Information provided by it, the scope of the information, the identity of the recipient of the information, the reasons for providing the information, whether the information was encrypted or protected by other security tools and any other relevant information, unless it is prohibited from doing so by statute.

4.9.5.1.2. The Provider will not take any action that may assist in decoding or removing any technological barrier from Protected Information in any way or form, by act or omission. If such a request for decoding or making accessible Protected Information is received from a law enforcement or security authority of a foreign country, the Provider will contact the Tender Administrator to get permission for providing such assistance and will follow the Tender Administrator's instructions.

4.9.5.1.3. If the Protected Information has been transferred without notifying the Tender Administrator, (whether an order preventing the disclosure of the request to send the information was issued, whether it is a demand of a security authority or for any other reason), the Provider will pay the Tender Administrator special compensation of NIS 7,555 within up to 24 hours from the time the information is provided.

4.9.5.2. Nothing in this section will derogate from the Provider’s responsibility, and its obligation under law and under the provisions of the Agreement not to provide Protected Information without the prior written consent of the Tender Administrator, nor will it derogate from any right to compensation, indemnification or any other remedy available to the Tender Administrator, as set forth in the Agreement.

5. Appendix C2 - information processing for services that are not in software as a service (non-SaaS) configuration

5.1. Protected information

5.1.1. Without derogating from the Provider's obligation elsewhere, if protected information is saved in the systems of the Provider, the Provider will be responsible for the safeguarding, protection and integrity of the protected information on its systems, and will not access it, will not allow any other party to access it, will not use or modify it, and will not permit any use or modification, by act or by default, which is not permitted according to the provisions of Israeli law, the provisions of the Agreement and this Appendix.

5.1.2. The Provider will be responsible for ensuring that Clients and users have regular access to the protected information, in accordance with its obligations under this Agreement, and in any case will not deny them access to such information, in a manner that contravenes the provisions of the Agreement or Israeli law.

5.1.3. The Provider understands that the protected information includes information about the work processes of the Government of Israel and information pertains in part to the citizens and residents of the State of Israel. Accordingly, any disclosure, compromising, damage, denial of access or loss of protected information or disclosure of information to a third party may cause the Tender Administrator, Clients, users and third parties heavy damage, and it will be required to safeguard the protected information in accordance with the highest standards existing in the marketplace, and will not transfer it to any third party, in accordance with the provisions of this Appendix.

5.1.4. Protected information will not be kept on public cloud infrastructure that is not one of the Cloud Providers winning the cloud tender.

5.1.5. The Provider's obligations in relation to the Protected Information will apply as long as the information is in its systems, even after the end of the engagement period.

5.1.6. Keeping of the documentation for a period of at least one year will be possible, meaning that it will be continuously available to the Client and to the Tender Administrator.

5.2. Content data

5.2.1. The Clients will be allowed to produce content data in or through the Provider's systems and to migrate to the Provider's cloud systems any content data as they wish, subject to the provisions of the law, including content data with differing levels of sensitivity, including content data of Clients that are subject to various statutory restrictions, for which the Provider will have no argument and will impose no restrictions.

5.2.2. Under the Israeli law applying to the content data of some of the Clients as updated from time to time, there are requirements regarding the protection of the information against defacement, alteration and unauthorized disclosure. The statutes that apply to information include the Regulation of Security in Public Bodies Law, 5758-1998, the Commercial Torts Law, the State Property Law, as well as specific statutes that apply to the activity of the state and government employees in various fields. The statutory obligations towards the Protected Information are imposed on the Clients only, which own the information, and not on the Provider, unless expressly stated otherwise in the tender documents. The Provider's duty is to make every reasonable effort to allow the Clients and the Tender Administrator to discharge the various statutory obligations applicable to them with respect to such Protected Information. Nothing in this section will derogate from any statutory obligation imposed on the Provider.

5.3. Use of Protected Information

5.3.1. The Tender Administrator and the Clients are the sole owners of the Protected Information, and the Provider constitutes a processor of the Protected Information and will not take any action, including saving and storage, processing of information and transfer thereof to any third party except in accordance with applicable statutes in the State of Israel and as set forth below:

5.3.1.1. For processing data – at the minimum level required for the correct provision of the services purchased under the Agreement, including improving the cyber protection of the Provider's systems or the services, for charging for them and discharging the Provider's obligations under the Agreement. It should be emphasized that the use of processing data for the purpose of improving the services of the Provider that is not part of the improvement of those services for, among others, the Clients, is prohibited except in the case of obtaining written permission from the Tender Administrator.

5.3.1.2. For access data – at the minimum level required for the proper delivery of the services purchased under the Agreement, for charging for them and for the meeting of the Provider's obligations under the Agreement.

5.3.2. Without derogating from the foregoing, and for the removal of doubt, the Provider will not sell, rent out or perform any other commercial operation using Protected Information, including the transfer of the information after processing, the transfer or sale thereof as part of other users' information after deleting identifying details, or in any other constellation.

5.3.3. The Provider will not store Protected Information on its systems other than in accordance with the provisions of the Agreement and this Appendix, and according to a digital instruction, and will ensure the purging of such information contained in its systems, according to statutory provisions.

5.3.4. Without derogating from the Provider's obligations, the Provider will take the necessary precautions to ensure that access to Protected Information is granted only to authorized employees of the Provider for whom access to this information is required for the provision of the services to Clients. The Provider must ensure that the disclosure and use of Protected Information to and by authorized parties will be to the minimum extent required for the purpose of providing the service properly, and in accordance with the Provider's obligations. The Provider will instruct the authorized parties on the purposes of the use of the information, and the obligations imposed on them by law and the provisions of hereof as a result of having the information disclosed to them.

5.3.5. **Deletion of Protected Information**

5.3.5.1. After the customer's use of the Service ends, subject to its statutory obligations, the Provider will delete from its records and databases all processing data and access data necessary for performing the permitted operations set forth in this section.

5.4. Confidentiality

5.4.1. The ~~provider~~Provider will be required to take all steps required of it for safeguarding the secrecy of access data and processing data that is saved in the Provider's system in a secret, secured manner, including undertaking as follows:

5.4.1.1. That this data will be saved using the most advanced technological means existing in the marketplace.

5.4.1.2. That access to this data by the Provider's employees will be only by authorized persons requiring this access, to the minimal extent required.

5.4.2. The Provider will be responsible for its sub-processors that will have access to Protected Information from it for providing the services to the Clients, will be bound to confidentiality as set forth in this Appendix, and in any case it will be fully responsible for any breach of this duty by them.

5.5. Criminal prohibition against disclosing Protected Information

5.5.1. Exposure or disclosure of confidential information under this Agreement, whether by act or omission, and which is not in accordance with the express, written consent of the Tender Administrator, constitutes a breach of the Provider's duty of confidentiality under this Agreement and constitutes a criminal offense under Section 118 of the Penal Law, 5737-1977.

5.5.2. In addition, depending on the type of information that is disclosed, disclosure of Protected Information, whether by act or omission, other than according to the provisions of the Agreement or statutory demands, may constitute a criminal offense under Israeli law, depending on the type of information disclosed (for example: Private Information, information that is privileged under Israeli law, information that could harm the state security of the state, etc.).

5.6. Applicable law and jurisdiction for Protected Information

5.6.1. **Without derogating from the statements in Section 3.34 of the Agreement:**

5.6.1.1. The State of Israel has a full, exclusive sovereign interest, and full powers over and ownership of the Protected Information. As such, the law that applies to Protected Information is the law of the State of Israel, and the courts of the State of Israel have exclusive jurisdiction to hear any question or proceeding concerning the said information, without qualifications or exceptions.

5.6.1.2. For any direct conflict between the Provider and the Tender Administrator in relation to the Protected Information, the applicable law will be Israeli law and the jurisdiction to hear any question or proceeding concerning the said information will be conferred exclusively to the courts of the State of Israel, without qualifications or exceptions.

5.6.2. The Provider will immediately announce any changes or updates in the legal situation applying to it that affects the exercising of the duties and rights in relation to the Protected Information under this Agreement. For the removal of doubt, such a change will not exempt the Provider of its obligations in accordance with the provisions of the Agreement.

6. Appendix D1 – Security and Cyber for Services in Software as a Service (SaaS) Configuration

6.1. Obligation of the Provider to information and cyber security

6.1.1. The Provider will be solely responsible for the security of the systems on which the services offered by it to Clients are based, whether directly, by a sub-processor or through a corresponding agreement with the provider of the cloud on which the service operates, will ensure the operation and update of the security measures on an ongoing basis, and will make sure that the technological means used for information security are state-of-the-art and comply with the highest standard practiced in the market.

6.1.2. The Provider will be responsible for protecting its systems, including dedicated infrastructure, as well as the services that it offers against cyber threats and attacks and any attempt to damage or block access to these infrastructures. As part of this, the Provider will monitor its systems and will work to detect and address weaknesses in its systems, and update its systems against security exposures as soon as possible, using mitigation processes, as long as the systems cannot be updated immediately.

6.1.3. The Provider will assign a representative who will be responsible for inquiries regarding information security and cyber protection, conducting audits, providing references as required by the Agreement, alerts on threats and coping with events in real time. If the service provider operates a situation room for coping with cyber threats (SOC), the representative will send the contact details of that situation room to the Tender Administrator.

6.1.4. The Provider's responsibility for information security and cyber protection will include, among other things, complying with the following principles, if relevant to the provision of the services:

1. **Personnel management and training** – ensuring that employees and contractor

2. **Supply chain and provider management** – defining and maintaining mechanisms whose

employees recognize and understand their responsibilities in the field of information security and cyber protection policies.

role is to manage the entire supply chain of the Cloud Provider to ensure the reliability of the infrastructures through which the services are provided.

3. **Resource management** – maintaining mechanisms for identifying and protecting organizational assets and information assets in the organization, including those of customers and of the Client.

4. **Management of security incidents suspected incidents** – maintaining means for managing, responding to and communicating information about security incidents.

5. **Identity and access authorizations management** – maintaining mechanisms to ensure that access to Protected Information, information processing resources, facilities and virtual environments are for authorized users only.

6. **Functional continuity and recovery** – ensuring the functional continuity of the cloud services, including disaster recovery while ensuring the credibility and reliability of information at all times.

7. **Encryption and key management** – maintaining secure operation of the Provider’s services by setting up and implementing appropriate cryptographic mechanisms.

8. **Maintaining security level evaluation mechanisms** – establishing and managing appropriate processes for testing key components in the network and information systems that support the cloud services and establishing and managing appropriate processes to assess

the level of protection of critical assets.

9. **Physical and environmental security** – maintaining measures to prevent unauthorized access to physical sites to prevent damage, loss, attrition, malfunction, or theft of organizational assets that may impair the Provider's activity.

10. **Maintaining migration capability and interoperability** – assigning the customer means that allow it to interface with other cloud services or migrate securely to providers that provide similar services.

11. **Maintaining secure operational functional continuity** – ensuring that the Provider's cyber protection apparatus operates securely and properly so that the cloud services are operational at all times.

12. **Protecting the integrity and reliability of the system** – establishing and managing the appropriate measures to ensure that the system maintains an adequate level of protection and reliability throughout its lifecycle, from development to operational deployment, including internal development and external development, using commercial and open-source tools.

13. **Communication security** – securing digital connection.

14. **Risk Management** – allocating the necessary measures for governance and information risk management, and mechanisms for identifying risks for protecting cloud services.

15. **Protection of personal information** – establishing and managing the necessary means for Clients to meet their obligations to protect the information under their control.

16. **Proper procedures for evaluating cyber protection** – establishing and managing proper processes, testing of security review procedures of systems and core networks of the cloud infrastructure.

17. **Configuration and change management** – establishing and managing change management for the network and information systems.

18. **Secure development** – establishing and managing the appropriate measures to ensure that the entire system development lifecycle is implemented using secure development methodologies, such as the SDLC methodology.

6.2. Cyber protection and risk management procedures

6.2.1. The Provider will establish cyber security procedures according to the Provider’s commitment to information security and cyber protection as set forth above, and to contend with ascribed scenarios and threats to the cloud infrastructures and services provided based on these infrastructures (hereinafter: the “**Provider’s Cyber Policy**”).

6.2.2. The Provider will perform, on an ongoing basis, risk management procedures in accordance with the requirements of the standards that it complies with and the requirements of the laws and regulations applying to it.

6.3. Standards

6.3.1. Acceptable international standards provide a minimum basic framework for the cyber protection infrastructure required by the Provider. The Provider must comply with accepted international standards in the field of providing the services that it provides.

6.3.2. Without derogating from the foregoing, an Israeli service will at least meet the standards that must be provided in the ~~temporary~~overseas region. If is not possible to obtain the relevant standard seal in Israel, the Provider must meet the requirements of the standard in full, even without receiving the official certification.

6.3.3. Upon the demand of the Tender Administrator, the Provider will present the official certification proving its compliance with the required standards. In the event providing official certification is not possible, the Provider will present the control process employed to meet the relevant standard, and upon the Tender Administrator’s demand, will present confirmation from an independent external body that has relevant qualifications, using commonly accepted methodology.

6.3.4. As these standards are updated or a new version released, the Provider will be required to update them accordingly.

6.3.5. The Provider will publicly update the devices for which the service has been certified.

6.4. Ongoing updates and information transfer on cyber threats

6.4.1. The Provider will cooperate with the Tender Administrator on the subject of protection against cyber threats, as part of the provision of the services, according to the following:

6.4.1.1. The Tender Administrator will provide, subject to the restrictions applying to it and the information disclosure policy that it will form, information that may assist in information security and cyber protection in accordance with the provisions of the Agreement, including information on cyber threats, methods, attack patterns and technologies that may be used against the Clients or the Provider in relation to the provision of the services to the Clients.

6.4.1.2. The Provider will transmit as soon as possible, subject to the restrictions applying to it and in accordance with any law, information that may assist the Clients and the Tender Administrator in information security and cyber protection, including information about cyber threats, methods, attack patterns and technologies that pose a threat to Protected Information and services purchased by Clients.

6.5. Coping with events in real time and incident investigation

6.5.1. The Provider will allow the Tender Administrator and the Clients to use investigation and IR (Incident Response) services of the Provider, if it offers them, for coping with security incidents and malfunctions or investigating and studying these incidents. If the Provider has no dedicated IR Team, the Provider will assist the Client in coping with the incident by using the company's engineering team or outside parties that it employs.

6.5.2. To the extent possible, the Provider will inform Clients in real time about security incidents, including cyberattacks and attempted cyberattacks against the Client's systems and the Provider's infrastructures on which the Clients' systems and data are operated.

6.6. Integrity of employees and suppliers

6.6.1. The Provider will carry out commonly accepted processes for examining the integrity level of its employees, subcontractors and its suppliers, while implementing a plan for locating and responding to security threats originating from an insider party.

6.6.2. **Sub-processors**

6.6.2.1. The Provider may meet the obligations imposed on it under the Agreement by means of ~~approved~~ sub-processors. All obligations imposed on the Provider under the Agreement, including this Appendix, will apply in full to the approved sub-processors. In any case of breach of the Provider's obligations by means of a sub-processor, the Provider will bear full responsibility for that breach.

6.6.2.2. **Instructions for employing a sub-processor:**

6.6.2.2.1. The Provider will limit the ability of the sub-processor to access the customer's information to the minimum required for providing the service or continuing to provide the service to Clients or end users. The Provider will deny the sub-processor access to the information for any other purpose.

6.6.2.2.2. The sub-processor and all parties authorized on its behalf to access Protected Information will sign a nondisclosure agreement that will comply with the confidentiality obligations applying to the Provider.

6.6.2.2.3. The sub-processor has complied with the duty set forth in Section 4.3.4 that stipulates that an employee may only access Protected Information when necessary, to the appropriate level of disclosure.

6.6.2.2.4. Sending of information to a sub-processor is not prohibited by law (such as law applying to privacy, etc.).

6.6.2.2.5. The Provider will conduct periodical audits of subcontractors that provide services to Clients.

6.7. Information security in services

6.7.1. The Provider will make sure that the level of protection and reliability of the services provided by it will be high and will be updated and upgraded throughout the engagement period. The Provider will not downgrade the level of protection of the services without first notifying the Tender Administrator.

6.7.2. All approved services will meet the relevant and commonly accepted information and cyber security standards. The Tender Administrator may request references for compliance with a particular service with such standards, and for services that do not yet meet official standard tests, the Provider will send the details of the internal tests and tests by third-party laboratories that have examined the level of service, including test methodologies and the certifications of the testers. The Tender Administrator will update its cyber policy regarding the approved services, among other things, based on the evidence sent by the Provider.

6.7.3. The Provider will not have any access for changing, exchanging or viewing of information about the Client's encryption keys, if any, and will not use them in any way without obtaining the prior written approval of the Tender Administrator.

6.7.4. The Provider will not prevent any use of the customer's cyber protection tools and measures required to secure the services, including the encryption mechanisms that it employs, insofar as this does not to impair the correct provision of the service.

6.7.5. Periodical audits

6.7.5.1. At a frequency depending on the Provider's risk management, or in response to the Tender Administrator's request and in coordination with the Provider, the Provider will conduct an external audit using an independent, leading company specializing in such auditing (hereinafter: the "**Audit Company**") to verify the Provider's compliance with the Tender provisions or will allow the Tender Administrator to perform such an audit. A request by the Tender Administrator for an external audit will be made at most once a year, except if it is in connection with a security incident. The Provider will discuss the audit reports that will be sent to it at the end of the audit and will examine the need to update the security procedure following them accordingly.

6.7.5.2. At the request of the Tender Administrator, and by advance notice to the Provider, the Audit Company will conduct a special audit, given a Security incident or changes in the Provider's security procedures and methods.

6.7.5.3. The Tender Administrator may demand information about the Audit Company, its certifications, and details about its auditors. The Tender Administrator may demand that the Provider replace the Audit Company, in cases of well-founded concern that the company is not performing its function as required.

6.7.5.4. At the request of the Tender Administrator, the Provider will send the Tender Administrator a summary of the audit findings and the status of the addressing the findings.

6.7.6. Security and penetration tests

6.7.6.1. The Tender Administrator may review control the implementation of its set policy for Clients and the manner in which it is implemented on the Provider's infrastructures.

6.7.6.2. This test will be performed both at the level of checking the settings and configuration of the systems as set by the Client and by performing resilience tests for the Client's systems operated on the Provider's systems and infrastructure.

6.7.6.3. To minimize the risks involved in these tests, the resilience tests will be arranged in advance with the Provider during which time the Provider will refrain from blocking the testing parties.

6.8. Cyberattack and security incident

6.8.1. In any case in which a cyberattack or any security incident has been detected in the Provider's systems that can affect the Clients, the Provider will take the following actions:

6.8.1.1. It will inform the Client and the Tender Administrator as soon as possible, depending on the severity of the incident, and in any case not more than ~~5~~12 hours from the moment it has confirmed the cyberattack incident, except in a case where an order is issued by a competent judicial court prohibiting it.

6.8.1.2. The Provider will take every necessary step, depending on the circumstances, to reduce the effects and minimize the damage resulting from the cyberattack.

6.8.1.3. The Provider will inform the Client and the Tender Administrator of the steps they can take to reduce the effects and minimize the damage resulting from the security incident.

6.8.1.4. The Provider will conduct an investigation of the attack incident and will send the findings of the investigation to the Client and the Tender Administrator for study. The investigation will include information according to the commonly accepted rules of information sharing in the cyber field.

6.8.2. The Provider will report, on an ongoing basis, to the Client and the Tender Administrator, on actions it has monitored as attempted cyberattacks targeting the Clients' systems.

6.8.3. The Provider will learn from the security incidents that have occurred and will examine the need to update the systems, processes and procedures.

6.8.4. In the event of a security incident having occurred in a Software as a Service type system, the Provider will indemnify the Client or the Tender Administrator, subject to clause 3.26.5, for any reasonable, documented expense that has been made to investigate, contain, reduce, limit and correct the breach of the Client's confidentiality, integrity and availability of information, including processes for notifying the relevant authorities of the incident.

7. Appendix D2 – Security and Cyber for Services that are not in Software as a Service (SaaS) Configuration

7.1. Obligation of the Provider for information and cyber security

7.1.1. The Provider will be solely responsible for the security of the systems on which the services offered by it to Clients are based, whether directly, by a sub-processor or through a corresponding agreement with the ~~provider~~Provider of the cloud on which the service operates, will ensure the operation and update of the security measures on an ongoing basis, and will make sure that the technological means used for information security are state-of-the-art and comply with the highest standard practiced in the market.

7.1.2. The Provider will assign a representative who will be responsible for inquiries regarding information security and cyber protection, conducting audits, providing references as required by the Agreement, alerts on threats and coping with events in real time. If the service provider operates a situation room for coping with cyber threats (SOC), the representative will send the contact details of that situation room to the Tender Administrator.

7.1.3. The Provider's responsibility for information security and cyber protection will include, among other things, complying with the following principles, if relevant to the provision of the services:

1. **Personnel management and training** – ensuring that employees and contractor employees recognize and understand their responsibilities in the field of information

2. **Supply chain and provider management** – defining and maintaining mechanisms whose role is to manage the entire supply chain of the Cloud Provider to ensure the reliability of the

security and cyber protection policies.

infrastructures through which the services are provided.

3. **Resource management** – maintaining mechanisms for identifying and protecting organizational assets and information assets in the organization, including those of customers and of the Client.

4. **Management of security incidents suspected incidents** – maintaining means for managing, responding to and communicating information about security incidents.

5. **Identity and access authorizations management** – maintaining mechanisms to ensure that access to Protected Information, information processing resources, facilities and virtual environments are for authorized users only.

6. **Encryption and key management** – maintaining secure operation of the Provider's services by setting up and implementing appropriate cryptographic mechanisms.

7. **Maintaining security level evaluation mechanisms** – establishing and managing appropriate processes for testing key components in the network and information systems that support the cloud services and establishing and managing appropriate processes to assess the level of protection of critical assets.

8. **Physical and environmental security** – maintaining measures to prevent unauthorized access to physical sites to prevent damage, loss, attrition, malfunction, or theft of organizational assets that may impair the Provider's activity.

9. **Risk Management** – allocating the necessary measures for governance and information risk management, and mechanisms for identifying risks for protecting cloud services.

10. **Protecting the integrity and reliability of the system** – establishing and managing the appropriate measures to ensure that the system maintains an adequate level of protection and reliability throughout its lifecycle, from development to operational deployment, including internal development and external development, using commercial and open-source tools.

11. **Communication security** – securing digital connection.

12. **Protection of personal information** – establishing and managing the necessary means for Clients to meet their obligations to protect the information under their control.

13. **Proper procedures for evaluating cyber protection** – establishing and managing proper processes, testing of security review procedures of systems and core networks of the cloud infrastructure.

14. **Secure development** – establishing and managing the appropriate measures to ensure that the entire system development lifecycle is implemented using secure development methodologies, such as the SDLC methodology.

7.2. Cyber protection and risk management procedures

7.2.1. The Provider will establish cyber security procedures according to the Provider’s commitment to information security and cyber protection as set forth above, and to contend with ascribed scenarios and threats to the cloud infrastructures and services provided based on these infrastructures (hereinafter: the “**Provider’s Cyber Policy**”).

7.2.2. The Provider will perform, on an ongoing basis, risk management procedures in accordance with the requirements of the standards that it complies with and the requirements of the laws and regulations applying to it.

7.3. Ongoing updates and information transfer on cyber threats

7.3.1. The Provider will cooperate with the Tender Administrator on the subject of protection against cyber threats, as part of the provision of the services, according to the following:

7.3.1.1. The Tender Administrator will provide, subject to the restrictions applying to it and the information disclosure policy that it will form, information that may assist in information security and cyber protection in accordance with the provisions of the Agreement, including information on cyber threats, methods, attack patterns and technologies that may be used against the Clients or the Provider in relation to the provision of the services to the Clients.

7.3.1.2. The Provider will transmit as soon as possible, subject to the restrictions applying to it and in accordance with any law, information that may assist the Clients and the Tender Administrator in information security and cyber protection, including information about cyber threats, methods, attack patterns and technologies that pose a threat to Protected Information and services purchased by Clients.

7.4. Coping with events in real time and incident investigation

7.4.1. The Provider will notify the Clients, to the extent possible in real time, about security incidents, including security vulnerabilities in services, a cyberattack against systems operated by other Clients and attempted cyberattacks against the infrastructures of the Provider used to provide the service or containing content data.

7.5. Integrity of employees and suppliers

7.5.1. The Provider will carry out commonly accepted processes for examining the integrity level of its employees, subcontractors and its suppliers, while implementing a plan for locating and responding to security threats originating from an insider party.

7.5.2. Sub-processors

7.5.2.1. The Provider may meet the obligations imposed on it under the Agreement by means of ~~approved~~ sub-processors. All obligations imposed on the Provider under the Agreement, including this Appendix, will apply in full to the approved sub-processors. In any case of breach of the Provider's obligations by means of a sub-processor, the Provider will bear full responsibility for that breach.

7.5.2.2. Instructions for employing a sub-processor:

7.5.2.2.1. The Provider will limit the ability of the sub-processor to access the customer's information to the minimum required for providing the service or continuing to provide the service to Clients or end users. The Provider will deny the sub-processor access to the information for any other purpose.

7.5.2.2.2. The sub-processor and all parties authorized on its behalf to access Protected Information will sign a nondisclosure agreement that will comply with the confidentiality obligations applying to the Provider.

7.5.2.2.3. The sub-processor has complied with the duty set forth in Section 4.3.4 that stipulates that an employee may only access Protected Information when necessary, to the appropriate level of disclosure.

7.5.2.2.4. Sending of information to a sub-processor is not prohibited by law (such as law applying to privacy, etc.).

7.5.2.2.5. The Provider will conduct periodical audits of subcontractors that provide services to Clients.

7.6. Information security in services

7.6.1. The Provider will make sure that the level of protection and reliability of the services provided by it will be high and will be updated and upgraded throughout the engagement period. The Provider will not downgrade the level of protection of the services without first notifying the Tender Administrator.

7.6.2. All approved services will meet the relevant and commonly accepted information and cyber security standards. The Tender Administrator may request references for compliance with a particular service with such standards, and for services that do not yet meet official standard tests, the Provider will send the details of the internal tests and tests by third-party laboratories that have examined the level of service, including test methodologies and the certifications of the testers. The Tender Administrator will update its cyber policy regarding the approved services, among other things, based on the evidence sent by the Provider.

7.6.3. **Periodical audits**

7.6.3.1. At a frequency depending on the Provider’s risk management, or in response to the Tender Administrator’s request and in coordination with the Provider, the Provider will conduct an external audit using an independent, leading company specializing in such auditing (hereinafter: the “**Audit Company**”) to verify the Provider’s compliance with the Tender provisions or will allow the Tender Administrator to perform such an audit. A request by the Tender Administrator for a special audit will be made at most once a year, except if it is in connection with a security incident. The Provider will discuss the audit reports that will be sent to it at the end of the audit and will examine the need to update the security procedure following them accordingly.

7.6.3.2. At the request of the Tender Administrator, and by advance notice to the Provider, the Audit Company will conduct a special audit, given a cyberattack or changes in the Provider’s security procedures and methods.

7.6.3.3. The Tender Administrator may demand information about the Audit Company, its certifications, and details about its auditors. The Tender Administrator may demand that the Provider replace the Audit Company, in cases of well-founded concern that the company is not performing its function as required.

7.6.3.4. At the request of the Tender Administrator, the Provider will send the Tender Administrator a summary of the audit findings and the status of the addressing the findings.

7.7. Cyberattack and security incident

7.7.1. In any case in which a cyberattack or any security incident has been detected in the Provider's systems that can affect the Clients, the Provider will take the following actions:

7.7.2. It will inform the Client and the Tender Administrator as soon as possible, depending on the severity of the incident, and in any case not more than ~~5~~12 hours from the moment it has confirmed the cyberattack incident, except in the case where an order is issued by a competent judicial court prohibiting this.

7.7.3. The Provider will take every necessary step, depending on the circumstances, to reduce the effects and minimize the damage resulting from the cyberattack.

7.7.4. The Provider will inform the Client and the Tender Administrator of the steps they can take to reduce the effects and minimize the damage resulting from the security incident.

7.7.5. The Provider will conduct an investigation of the attack incident and will send the findings of the investigation to the Client and the Tender Administrator for study. The investigation will include information according to the commonly accepted rules of information sharing in the cyber field.

7.7.6. The Provider will report, on an ongoing basis, to the Client and the Tender Administrator, on actions it has monitored as attempted cyberattacks targeting the Clients' systems.

7.7.7. The Provider will learn from the security incidents that have occurred and will examine the need to update the systems, processes and procedures.

Appendix E – Hebrew Agreement (will only be attached if the English version of the agreement is signed)