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. 2: Chapter 2 – The Bid Booklet

Version ~~2 – September~~3 – November 2022[*]

[*] *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.*

2. Chapter 2 - the Bid Booklet

2.1. General guidelines for the bidder's response to the Tender

2.1.1. This chapter constitutes the bidder's response to the Tender and there is no need to give a response to any other part of the Tender, or to attach a document that is not required in this chapter.

2.1.2. If the Bidder offers services from different manufacturers (as such are defined below in Appendix 6), this booklet is to be submitted separately for each manufacturer. In any other case, the Bidder is required to submit this booklet for all the services offered by it.

2.1.3. The guidelines given in this chapter must be carefully followed in order for the bid to be examined and evaluated properly. Bidders may not add to, delete or alter any of the terms of the Tender, or the guidelines below, nor subject them to any conditions.

2.1.4. In any case of questions or ambiguity in the tender documents, the bidder must contact the Tender Administrator with a question for clarification, as set forth in Chapter 1 of the tender documents. By submitting a bid as part of the Tender, the bidder accepts the terms of the Tender, and it will be barred from making any arguments against the Tender Administrator regarding these conditions.

2.1.5. Unless expressly stated otherwise, information and details beyond those required in this appendix may be added. Lack of details in a bid or a breakdown that does not meet the requirement may result in a low score of the bid or its disqualification at the sole discretion of the Tender Administrator. Nonetheless, there is no need to go into excessive detail, and it is advisable to keep a bid accurate and concise.

2.1.6. **List of documents to be submitted**

2.1.6.1. A response to the bid booklet set forth in this chapter including appendices in the following formats:

2.1.6.1.1. A filled digital source file in PDF format, digitally signed as required by the bidder's authorized signatories.

2.1.6.1.2. An identical digital copy in Word format **(not a scanned document)**.

2.1.7. Instructions for bids submission

2.1.7.1. Submission of bids for the Tender will be done online, according to the guide published on the Tender page, which also include a link to the bidding system.

2.1.7.2. As part of the submission process, the bidder must follow the instructions that will appear in the bidding system, fill in all the required fields, clearly and in accordance with the system's directions, and upload to the system all files required according to the Tender instructions.

2.1.7.3. The bidder in the Tender is responsible for making sure to submit the bid before the closing date. In this regard, the bidder must take into account that near the closing date, there may be an increased traffic volume on the submission system or other technical difficulties that will prevent the bidder from submitting its bid. It is the responsibility of the bidder to submit its bid a sufficient time before the closing date, in order to avoid such faults.

2.1.7.4. To the extent that several bids are submitted by the same bidder (in respect to the same service), the bid submitted last will be the only one reviewed.

2.1.7.5. Bids submitted after the closing date, will not be accepted for evaluation.

2.1.8. Closing Date of the Tender

2.1.8.1. The Closing Date of the Tender for the categories listed in section 2.3 below, is **December 15, 2022 at 17:00 (Israel Standard Time)**.

2.2. Bidder's information

1.	**Name of the bidder** (as listed in the relevant register)	
2.	**Type of incorporation** (for example – a limited liability company / private company, etc.).	
3.	**Place of incorporation of the bidder** – state the country in which the association is registered.	
4.	**Registration date**	
5.	**Identifying number**	
6.	**Details about activities in Israel** (if An Israeli corporation or a corporation without an Israeli representation, does not need to fill this in)	Is the corporation registered in Israel as a foreign company- Registration number – Date of registration –
		Name of representation unit in Israel (if any):
		Type of representation unit (subsidiary, concessionaire, division, etc.):
		Powers of the representation unit in Israel:
7.	**The contact person on behalf of the bidder for the purpose of the Tender**	Name:
		Address:
		Telephone:
		Email:

2.3. List of categories

2.3.1. At this time, bidders for this Tender are allowed to submit for the Tender a service or services in the following categories:

GCP - Marketplace	AWS - Marketplace
Analytics	Data analytics
Developer tools	Application development

2.3.2. If a service is available in one of the above categories of one of the Cloud Providers, it may be submitted in the tender for both Cloud Providers

2.4. Requirements applying to an Israeli bidder (to be filled in by an Israeli bidder only)

A bidder that it is a company registered in Israel or that has an active registered representation unit in Israel is required to specify its compliance, as set forth in Sections 2.4.1~~2.4.1~~-2.4.3~~2.4.3~~, as set forth below.

2.4.1. **Bookkeeping – the bidder declares that:**

2.4.1.1. The bidder, or its Israeli branch, maintains account ledgers and records that it must maintain in accordance with the Income Tax Ordinance and the Value Added Tax Law, 5736-1975 (the "Value Added Tax Law"), or is exempt from maintaining them.

2.4.1.2. The bidder, or its Israeli branch, reports its income to the Assessment Officer and reports transactions that are taxed under the Value Added Tax Law to the Director, or is exempt from it doing so.

For the purpose of proving compliance with this condition, the bidder must submit Appendix 1.

2.4.2. **Absence of convictions**

2.4.2.1. The bidder or its Israeli branch and an "affiliate" thereof (as defined in Section 2B of the Public Bodies Transactions Law), have not been convicted of more than two offenses under the Foreign Workers Law 5751-1991 (hereinafter: the "**Foreign Workers Law**") and the Minimum Wage Law, 5747-1987 (hereinafter: the "**Minimum Wage Law**") by the Closing Date, or have been convicted as aforesaid but at least one year has elapsed from the date of the last conviction to the Closing Date.

For the purpose of proving compliance with this condition, the bidder must submit an affidavit regarding the absence of convictions as set forth in Appendix 2.

2.4.3. **Adequate representation for persons with disabilities (check X at one of the options)**

The bidder, or its Israeli branch, meets the requirements of Section 2B1 of the Public Bodies Transactions Law, regarding adequate representation for persons with disabilities, as in the following manner (***check X at the appropriate box***):

□ The provisions of Section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 do not apply to the bidder.

□ The provisions of Section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 apply to the bidder and it complies with them.

1) (If the provisions of Section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998 **apply to the bidder,** checking the appropriate box is required):

□ The bidder employs less than 100 employees.

□ The bidder employs at least 100 employees.

2) (If the bidder employs at least 100 employees, checking in the appropriate box is required):

□ The bidder warrants that if it wins the Tender, it will contact the Director General of the Ministry of Labor, Social Affairs and Social Services to review the implementation of its duties under Section 9 of the Equal Rights for Persons with

Disabilities Law, 5758-1998, and if necessary – for instructions on how to implement them.

□ The bidder previously undertook to contact the Director General of the Ministry of Labor, Social Affairs and Social Services to examine the implementation of its duties under Section 9 of the Equal Rights for Persons with Disabilities Law, 5758-1998, it contacted the Ministry as set forth, and if it received instructions for implementing its duties, **acted to instructed** (if the bidder previously undertook to contact the Director General and an engagement was made with it, for which it gave that undertaking).

□ The bidder undertakes to send a copy of this affidavit to the Director General of the Ministry of Labor, Social Affairs and Social Services within 30 days from the date of the engagement.

2.4.4. Rights in the offered service - the Bidder declares that it holds the full rights to sell the offered service in the Government Digital Marketplace, and to undertake the requirements of the tender.

For the purpose of proving compliance with this condition, the Bidder is required to attach Appendix 6.

2.5. General obligations of a bidder

2.5.1. Declarations of the bidder with the submission of the bid

2.5.1.1. The bidder has carefully read the tender documents, including all chapters, appendices, terms and parts, including all the clarifications published by the Tender Administrator, has understood everything stated therein and consents thereto.

2.5.1.2. The bidder has carefully read the terms of the engagement with the winning provider, including the engagement contract and its appendices, it has understood everything stated therein and consents thereto.

2.5.1.3. The bidder is not in bankruptcy or liquidation proceedings and no material legal proceedings are being conducted against the bidder that may impair its functioning if it wins the Tender.

2.5.1.4. There is no statutory impediment to the bidder's participation in the Tender.

2.5.1.5. The submission of a bid in the Tender or the execution of the engagement that is the subject of the Tender by the bidder does not form conflict of interest, either directly or indirectly, between the bidder and the Tender Administrator.

2.5.1.6. This bid is being submitted in good faith.

2.5.2. Non-coordination of bids in the Tender

2.5.2.1. The details appearing in the bid were decided on by the bidder independently, without consultation, arrangement or contact with any other bidder.

2.5.2.2. The bid details have not been and will not be shown to any person or corporation making bids in this Tender.

2.5.2.3. The bidder was not involved in any attempt to dissuade another contender from submitting bids in this Tender.

2.5.2.4. The bidder has not been and does not intend to be involved in an attempt to get another contender to submit a bid higher or lower than its own bid.

2.5.2.5. The bidder has not been involved in any attempt to get a contender to submit a non-competitive bid of any kind.

2.5.3. Woman-controlled business

2.5.3.1. A bidder that it is a "woman-controlled business" and that wishes to be given preference as such is to attach to its bid a confirmation and an affidavit, in accordance with the provisions of Section 2B of the Mandatory Tenders Law, 5752-1992.

2.6. Parts of the bid that the bidder seeks to keep confidential

2.6.1. The following are the pages, sections or documents included in the bid that the bidder believes that their disclosure constitutes an exposure of a trade secret or professional secret.

Page / Section Number	**Subject of the section**	**Rationale for preventing disclosure**

2.7. Confirmation of the bidder (digitally signed)

2.7.1. By signing we confirm that:

We have read all the provisions of the Tender, we understand and accept every clause in the Tender, the bid is being submitted in accordance with the conditions of the Tender, and meets its conditions, and the bidder will be barred and estopped from making arguments against the terms of the Tender from the moment of submitting this bid.

The details that appear in this bid and its appendices, are true, and the bidder is able and intends to meet every detail of its bid and the provisions of the Tender.

Date	Full name	Signature of the Provider's authorized signatory **Digital signature**
Date	Full name	Signature of the Provider's authorized signatory **Digital signature**

2.8. List of appendices that are to be attached to the bid

Appendix No.	Appendix name	Directions for answering the appendix
Appendix 1	**Confirmation of compliance with the Public Bodies Transactions Law**	A valid confirmation from an "authorized officer" under the Public Bodies Transactions Law of keeping of account ledgers, and a valid confirmation from an "authorized officer" of reporting to the tax authorities as required by law are to be attached. **** For a bidder that is a company registered in Israel or has an active representation unit in Israel.**
Appendix 2	**Attorney affidavit regarding the absence of convictions under the Public Bodies Transactions Law**	The bidder must attach an attorney affidavit worded as stated in in Appendix 3. **** For a bidder that is a company registered in Israel or has an active representation unit in Israel.**
Appendix 3	**List of services offered in the AWS and GCP digital marketplace and that are submitted in this tender**	The bidder must list in this appendix the services included in the digital marketplace of the Cloud Providers and that are being offered by it as part of this Tender, according to the breakdown in the appendix.
Appendix 4	**Unique requirements in cyber protection, privacy and additional issues in the information security field – answer guide**	
Appendix 4.1	**Unique requirements in cyber protection, privacy and additional issues in the**	The bidder must provide in this appendix a detailed answer to all the requirements for each of the services offered by it.

Appendix No.	Appendix name	Directions for answering the appendix
	information security field for Software as a Service (SaaS) services	
Appendix 4.2	**Unique requirements in cyber protection, privacy and issues in the information security field for Non-SaaS services**	The bidder must provide in this appendix a detailed answer to all the requirements for each of the services offered by it.
Appendix 5	**Price quotation**	The bidder must submit the price quotation according to the directions in the tender documents.
Appendix 6	**Manufacturer statement**	The Bidder should submit the Manufacturer's statement in accordance with the instructions specified below in this appendix.

Appendix 1 – Confirmation of compliance with the Public Bodies Transactions Law

A valid confirmation from an “authorized officer” under the Public Bodies Transactions Law of keeping of account ledgers, and a valid confirmation from an “authorized officer” of reporting to the tax authorities as required by law are to be attached. To this end, the following link may be used: confirmation of withholding tax at source

Appendix 2 – Affidavit on absence of convictions under the Public Bodies Transactions Law

I, the undersigned, _________, Identity No. _____________, after having been warned that I must state the truth and will be liable for the penalties prescribed in the law should I fail to do so, hereby declare as follows:

I am giving this affidavit on behalf of ____________________, which is the bidder (hereinafter: the "**Bidder**") that wishes to engage with the Tender Administrator of tender No. 01-2022 for the addition of services to the Government Cloud Marketplace. I declare that I am authorized to give this affidavit on behalf of the Bidder.

In this affidavit, the meaning of the term "**affiliate**" is as defined in the Public Bodies Transactions Law 5736-1976 (hereinafter: the "**Public Bodies Transactions Law**"). I confirm that the meaning of this term has been explained to me and that I understand it.

The meaning of the term "**offense**" – an offense under the Foreign Workers Law (Prohibition of Unlawful Employment and Ensuring Fair Conditions), 5751-1991, or under the Minimum Wage Law 5747-1987, and in the case of transactions for receiving a service, as defined in Section 2 of the Increasement of Enforcement of Labor Statutes Law, 5772-2011, also a violation of the provisions of the statutes listed in the third addendum to that law too.

The Bidder is a corporation registered in Israel. (Check X in the appropriate box)

□ The Bidder and its affiliate **have not been convicted** of more than two offenses through to the Closing Date (hereinafter: the "**Closing Date**") for Tender 01-2022 for the addition of services to the Government Cloud Marketplace.

□ The Bidder or its affiliate has **been convicted** in a court ruling of more than two offenses and at least **one year has** elapsed from the date of the last conviction to the Closing Date.

□ The bidder or its affiliate has **been convicted** in a court ruling of more than two offenses and **one year has not elapsed** since the date of the last conviction to the Closing Date.

This is my name, below is my signature and the content of my affidavit above is the truth.

______________________	__________________	___________________
Date	Name	Signature and stamp

Attorney's Confirmation

I, the undersigned, ________________________, Adv., confirm that on the date of ____________, Mr. /Ms. _________________, who identified himself/herself by Identity Card No. ____________/ who is known to me personally, appeared before me at my office at the address ____________ in the town / city ____________, and that after I warned him/her that he/she must declare the truth and that would be liable for the penalties prescribed in the law should he/she fail to do so, signed the affidavit above before me.

__________________	____________________	____________________
Date	License No.	Signature and stamp

Appendix 3 – the Services Offered by the Bidder

2.9. Guidelines for how to reply to this appendix

2.9.1. The bidder must list in the table below all of the services that it wishes to offer under this Tender.

2.9.2. For each service, the bidder is to state the name of the service, restrictions or limitations for its use in the Israeli region, if any, and attach a link to the service page in any of the Cloud Provider’s marketplace.

2.9.3. If the service offered includes a number of service levels with different security characteristics, they should be specified as different services and each service level should be addressed separately.

2.9.4. All services must meet all the requirements of this Tender, and in particular the requirements set forth in Appendices 4 and 5.

2.10. List of services offered by the bidder

* Do not fill in this appendix in handwriting.

** Rows may be added as necessary in the same format as of the table.

*** For Non-SaaS service, if the service may be consumed using the digital marketplace of two Cloud Providers in an overseas region, **the service must be offered under this tender for the governmental digital market of both Cloud Providers.**

#	Name of the manufacturer and service (as it appears in the digital marketplace of the Cloud Provider) and link to the service page		Category within the digital marketplace of the Cloud Provider that the Service is included in		Type of Service (Circle the type of service – whether SaaS or non-SaaS)	The Cloud Provider on which the service in the governmental digital marketplace will be based		Does the service price include support? (elaborate)
	AWS	GCP	AWS	GCP				
					SaaS / Non-SaaS	□ AWS	□ GCP	
					SaaS / Non-SaaS	□ AWS	□ GCP	

Appendix 4 – Unique requirements on cyber protection, privacy and other issues in the information security field – answer guide

2.11. Guidelines for how to respond to this appendix

2.11.1. This appendix contains a list of requirements and questions in relation to the services offered in terms of cyber, privacy protection and other aspects of information security. Based on this response, the services as stated in Section שגיאה! מקור ההפניה לא נמצא.~~1.3.2~~ to the Tender documents will be evaluated.

2.11.2. The bidder must answer one of the two appendices, 4.1 or 4.2, according to the service it is offering (SaaS or non-SaaS) (accordingly).

2.11.3. This appendix must be submitted for each service separately. if there are several services for which the response to this appendix is the same, they can be submitted together in one appendix

2.11.4. The bidder is required to elaborate, as necessary, in the information provided, so that the Tender Administrator will have all the necessary information to evaluate and score its bid. In this regard, if the bidder is using sub-processors, the bid should cover all of the actions that will be done by the sub-processors.

2.11.5. The definitions appearing at the beginning of the Tender apply to professional terms appearing in this chapter (if any), in order to answer the questions accurately.

2.11.6. More information than required may be added, such as: creative suggestions and solutions, pointing out requirements that are made superfluous given the bidder's proposed answer or stating missing requirements, etc., provided that in the end, a clear answer to the requirements will be given, the main features of the proposed solution are emphasized, and it will be clear what exactly is being offered, what already exists and what is expected to exist in the future.

2.11.7. If a bidder attaches ancillary documents to its bid to meet the requirements of the appendix, it must do the following:

2.11.7.1. The bid must contain no links or references to external documents, and all relevant files are to be included as part of the bid.

2.11.7.2. References to ancillary documents from the relevant section in the appendix must be provided as an answer to or comments on the requirements of that section.

2.11.7.3. Any ancillary document attached to the bid must be marked with ascending numbering in the format of the appendix number and serial numbering. Examples: ancillary documents that are intended to provide an answer to the sections in Appendix 4 will be numbered as in the following manner: Ancillary Document 4.01, Ancillary Document 4.02 and so on.

2.11.7.4. An index for all ancillary documents attached to the bid must be attached, containing a reference to the appendix and the section to which they refer, in the following format (example):

Ancillary document number	The title of the ancillary document	The section in the tender documents to which the ancillary document refers
4.02	Supply chain security procedure	2.11.12.2

2.11.8. A lack of an answer, an answer that does not respond to the requirement, the lack of a response to a requirement, failure to refer to an ancillary document, attachment of unmarked documents or an unclear and unequivocal answer, may result in a low score or disqualification of the bid at the sole discretion of the Tender Administrator.

2.11.9. The answer to this appendix can be submitted in English.

Appendix 4.1 – requirements and questions regarding cyber protection, privacy and other issues in the field of information security for Software as a Service (SaaS)

Serial no.	Name of the Service for which this appendix is filled
1	
2	

(Rows may be added if necessary)

2.11.10. **The proposed service work configuration**

2.11.10.1. The bidder is to specify the configuration of the proposed service operation, covering the following points:

2.11.10.1.1. The location at which protected information is stored – in the "network" (such as VPC) of the Client, within the bidder's premises or anywhere else. If the information is not stored at the Client's premises, its storage location must be specified.

2.11.10.1.2. Content data processing location – in the "network" (such as VPC) of the Client, within the bidder's premises or anywhere else. If the content data is not processed at the Client's premises, its storage location must be specified.

2.11.10.1.3. If the material is stored and processed on the Client's premises, the bidder's ability to access or control the information or system, if any, must be specified.

2.11.10.1.4. The bidder is to specify the configuration of the system's connection to the Client's network, covering the following points:

2.11.10.1.4.1. The way in which the client network is connected in the cloud (such as VPC), specifying whether the connection is, for example in VPC, Endpoint or Peering configuration, the service is represented in the client network itself, via a VPN connection or otherwise, the way in which the connection is secured and whether external addresses must be opened to connect to the service.

2.11.10.1.4.2. The interface to the service management system, specifying whether the connection, is for example, in VPC endpoint or peering configuration, whether the service is represented in the client network itself, through a VPN connection or otherwise, the way in which the connection is secured and whether external addresses must be opened to connect to the service.

2.11.11. **Human capital security**

2.11.11.1. The Bidder is to describe the review, verification and vetting processes carried out for provider employees and subcontractors, covering the differences in processes according to the types of employees and the risk levels their positions entail.

2.11.11.2. The Bidder is to describe the initial and refresher training processes for security, protection and cyber procedures for Provider and subcontractor employees.

2.11.11.3. The Bidder is to describe the professional training and qualification processes for the professionals and subcontracting providers.

2.11.11.4. The Bidder is to describe the mechanisms for supervising compliance with the procedures and the way of dealing with violations of security procedures or other critical procedures.

2.11.11.5. The Bidder is to specify whether tools are used to detect human risks (such as detecting behavioral irregularities, feedback from supervisors or colleagues about problems, etc.) of functionaries in sensitive positions or with high access authorizations.

2.11.12. **Supply chain security**

2.11.12.1. All supply chain security processes and procedures are to be in accordance with standards approved for the Provider by the US Government, if any, or at level of security corresponding with common practice.

2.11.12.2. The Bidder is to specify the standard used for securing the supply chain, such as NIST SP 800-53 Rev. 5/Nist SP 800-161 Rev. 1, ISO 28000, another international standard, or attach the internal procedure as addendum, if applicable.

2.11.12.3. The Bidder is to describe the supply chain security measures, including the following topics:

2.11.12.3.1. The processes for reviewing the introduction of software from an external source and the updates thereto, including locating backdoors or planting of offensive capabilities.

2.11.12.3.2. The processes for reviewing the introduction of software from an internal source and the updates thereto, including locating backdoors or planting of offensive capabilities.

2.11.12.3.3. The Bidder is to describe any other relevant process or review.

2.11.12.4. The Bidder is to describe the process of oversight and review of all external providers, including the standards by which the review is carried out.

2.11.13. **The information stored on the Bidders' premises**

2.11.13.1. The bidder is to specify the information stored on its premises during the provision of the services, such as processing data or access data.

2.11.13.2. The bidder is to specify the information retention policy as well as the mechanisms used to delete the information when required.

2.11.13.3. If data is stored at the Provider's premises, the bidder is to specify the means of protecting the information and the tools and processes used to prevent unauthorized access to the information.

2.11.13.4. The bidder is to specify the process of granting access to this data and the user groups that are authorized to view the information and the review processes for detecting misuse of these authorizations.

2.11.14. **Configuration security and change management**

2.11.14.1. The Provider will follow an orderly policy for managing configuration and changes of all the systems participating in the provision of the services, in accordance with commonly accepted and required standards.

2.11.14.2. The Provider is to specify the standard by which these processes are performed, if any, providing a schematic description of the configuration control systems and the process of reviewing, approving and documenting the changes.

2.11.14.3. The bidder is to specify controls to prevent unauthorized downgrade of encryption mechanisms, key management mechanisms, protection systems and protection services, if any.

~~2.11.14.3.~~2.11.14.4. The manner of protection and reviewing the development processes is to be specified, including a secure development process (SDLC) and relevant standards, if the bidder complies with them.

2.11.15. **Restriction of support access**

2.11.15.1. The bidder is to specify the system support process, the identity of the supporting parties, whether the parties on behalf of the Provider or the Cloud Provider and the process implemented by the Provider in case of need for such access, including internal approval routes, approval processes with the customer, access security, the manner of documentation (including session recordings, if any), etc.

2.11.15.2. The bidder is to specify whether it is possible to implement a mechanism in which any support access to components used by the Client and containing or allowing access to processing data will be made only after the implementation of a defined approval process within which the Client’s representative must provide approval for the support access.

2.11.15.3. Any such access, or unauthorized access attempt, will be recorded in a systematic log, including the details of the accessing entity, the details of the approver and any other relevant data. This log will be accessible to the Client.

2.11.16. **Risk management**

2.11.16.1. If the bidder employ an information security manager who is responsible for the information security of the services offered, the bidder should specify the job description and whether this person is a member of the bidder's management.

2.11.16.2. The bidder is to specify the risk management processes in the organization.

2.11.16.3. The bidder is to specify the parties that perform these processes, the levels of supervision, the levels of escalation to deal with issues and the manner of dealing with unresolved findings.

2.11.16.4. The bidder is to specify the tools, means and their manner of implementation in order to provide for risk management in a dynamic manner and in accordance with changes in the different threats and the services provided by the Provider.

2.11.17. **Login for the offered service**

2.11.17.1. The service must support standard login protocols such as SAML, OpenID, OAuth, for single sign on with the Client's systems includes support for Multi Factor Authentication. The bidder is to specify the supported login protocols, the ability to interface with idP / IAM tools (such as user management systems of the cloud providers and with third-party systems such as OKTA, OneLogin, Azure AD), supported protocols (such as U2F, FIDO, OTP), etc.

2.11.17.2. The bidder is to specify support for granting access individually at the RBAC – Role Based Access Control, and at the ABAC – Attribute Based Access Control level.

2.11.17.3. The service must support the receipt of user details from a central login system using standard protocols.

2.11.18. **Business Survival and Continuity (SLA) of the offered service**

2.11.18.1. The SLA for the service that will provided from the Israeli region will not fall short of the SLA of any other region of the Provider.

2.11.18.2. The bidder must list the mechanisms that ensure the resiliency of the service and information, including the deployment of the system between different zones, the way in which the information is backed up, how the integrity of the backup is maintained, how restoration ability is tested, withstanding various failure scenarios, etc.

2.11.18.3. If the bidder performs backups outside the cloud environment, it must specify the mechanism that verifies the destruction of a memory medium and components that have reached the end of their service (such as their withdrawal from the system, replacement or in the case of a malfunction).

2.11.18.4. The bidder is to specify the manner of controlling the quality of the service provided from the Israeli region and the levels of escalation defined in the bidder’s procedures.

2.11.18.5. The bidder will allow the Client to back up and to export the **content data** to the platform controlled by the bidder on a regular basis. The bidder is to specify the backup format and its compatibility with standard systems in the market.

2.11.19. **Protection of the Provider’s infrastructures used for providing the offered services**

2.11.19.1. The Provider will operate a SOC that will monitor its systems in cyber aspects at least eight hours a day, five days a week. The bidder is to specify Provider-operated SOC operation times and capabilities, the SIEM system that it uses, and other components and capabilities used by the SOC in its day-to-day operation. As the SOC operated by a 3rd party, the bidder is to specify the 3rd party details.

2.11.19.2. The bidder is to specify the use of automation tools for monitoring and dealing with events, its methodology of operation (such as SOAR), the relevant tools and the way they are implemented.

2.11.19.3. Inbound and outbound traffic to and from the Provider’s network will be monitored to detect attacks or suspicious activity. The bidder is to specify its capabilities in this field and the work processes that it implements to this end.

2.11.19.4. The provider will implement monitoring and workflow processes with a Privacy by Design configuration, involving minimal exposure of information to human elements. The Bidder is to specify the tools and methods that it is applying to implement these processes.

2.11.19.5. The provider will use tools for continuous attack surface management (monitoring) – all the tools and the work processes used by the bidder must be specified.

2.11.19.6. The bidder is to specify the means used to protect the systems providing the services against unauthorized changes and the monitoring means it employs for reviewing this.

2.11.19.7. The bidder is to specify the manner of segregation and differentiation of common services and the means to prevent information leakage between different Clients, the access of resources of another Client, the separation of management and control, etc.

2.11.19.8. The Provider must ensure that all provider infrastructures, systems and services that it offers are updated with all relevant security updates. The update processes and frequency of performing updates must be specified.

2.11.19.9. All users belonging to the Provider or subcontracting providers that can access protected information or that have high access authorizations (privileged access) such as: administrators, operators, support, DevOps, etc., will be monitored and will have high-level authentication. The Provider must specify work processes and tools that it implements to this end.

2.11.19.10. The bidder is to specify the manner in which Clients' processing and access data is protected, including access control, encryption and security tools that protect against unauthorized access or leakage.

2.11.19.11. The bidder is to specify the manner of protection of system administration interfaces, segregation of users, and denial of access by unauthorized parties, including the Provider's employees and subcontractors.

2.11.19.12. The bidder is to specify the manner of protection of its API interfaces, internal and external.

~~2.11.20. **Configuration security and change management**~~

~~2.11.20.1.~~2.1.1.1. ~~The bidder is to specify controls to prevent unauthorized downgrade of encryption mechanisms, key management mechanisms, protection systems and protection services, if any.~~

~~2.11.21.~~2.11.20. **Security tools used for protecting the offered services**

~~2.11.21.1.~~2.11.20.1. The bidder is to specify advanced, automated analysis tools, including AI-integrated tools, to detect suspicious activity in users' services, attempted or actual exposure of sensitive information, etc.

~~2.11.21.2.~~2.11.20.2. The bidder is to specify additional cyber control, monitoring and protection tools that it uses, which will be available for use by the Clients to improve the protection of their information, such as DLP capabilities, dealing with malicious code, etc.

~~2.11.22.~~2.11.21. **Encryption and key management of the offered services**

~~2.11.22.1.~~2.11.21.1. The bidder is to specify the encryption capabilities for information in the various service layers.

~~2.11.22.2.~~2.11.21.2. The bidder will allow for encryption of all content data, if any, by default at rest and at transit.. If by the judgment of the bidder, this encryption is infeasible, this must be elaborated on in full, including compensatory controls, if any.

~~2.11.22.3.~~2.11.21.3. The bidder is to specify the encryption types and algorithms it uses in its services, such as at rest, in transit, and runtime, the standard on which they are based, and external references for algorithmic resilience and encryption protocols.

~~2.11.22.4.~~2.11.21.4. The bidder is to specify the manner of managing and storing the keys in relation to each of the different service layers and the various types of services.

~~2.11.22.5.~~2.11.21.5. All of the Provider's key management infrastructures, such as KMS and HSM, will fully comply with FIPS-140-2 level 2 standard. The bidder is to specify the plan for adapting its services to the FIPS-140-2 Level 3 standard if it does not comply with it currently. In addition, the bidder is to elaborate on its preparations for the FIPS 140-3 standard, if any.

~~2.11.22.6.~~2.11.21.6. The bidder is to state its abilities to work in Bring Your Own Key configuration, including the ability to protect the system, its hardening and the user's ability to control various parameters of the encryption keys.

~~2.11.22.7.~~2.11.21.7. The bidder is to specify the support for using the Client's HSM hosted on the Client's premises for managing the encryption keys.

~~2.11.22.8.~~2.11.21.8. All processes of generation, alteration, substitution, cancellation, etc. will be performed by the Client without the Provider or any other party that has not been permitted by the Client having any viewing or access ability (except for the services that needs access to the key itself for their operations).

~~2.11.23.~~2.11.22. Logging and monitoring

~~2.11.23.1.~~2.11.22.1. The Client may receive all data in regards to processing and access to its systems with support of transfer of the data to the SIEM systems of the Client, the Tender Administrator or to a third party. The bidder is to specify the manner of transferring the logs (online interface, periodic file transfer, API, etc.), the supported SIEM systems and the scope of support.

~~2.11.23.2.~~2.11.22.2. The bidder is to specify possible log sources (such as: infrastructure, applicative infrastructure, application, information security, etc.).

~~2.11.23.3.~~2.11.22.3. The bidder is to specify the currency of the information (the time from the occurrence of the event to the transfer of the information), the scope of the information, the ability of the Client or its representative to investigate it, etc.

~~2.11.23.4.~~2.11.22.4. The bidder is to specify the time for which the Provider keeps processing data and access data, the Provider's policy relating to the storage of this data and how it is protected.

~~2.11.24.~~2.11.23. Investigation

~~2.11.24.1.~~2.11.23.1. The bidder must specify its abilities and work processes in the field of cyber incident investigation.

~~2.11.24.2.~~2.11.23.2. The bidder must specify the tools and services available to the Clients for analysis, investigation and responding to cyber incidents.

~~2.11.24.3.~~2.11.23.3. The bidder is to specify the process of activating the incident response apparatus, if applicable, in case of need to investigate a security incident, the involvement of the Cloud Provider, response times, the resources accessible to the Client, the configuration of the interface, etc.

~~2.11.25.~~2.11.24. Internal review and compliance with standards

~~2.11.25.1.~~2.11.24.1. The service must comply, at the very least, the following standards:

~~2.11.25.1.1.~~2.11.24.1.1. ISO27001 or SOC 2 AICPA standard. The bidder is to specify the standard that it complies with.

~~2.11.25.1.2.~~2.11.24.1.2. The bidder is to specify additional standards that it complies with, such as: ISO27017, ISO27018, CSA STAR level 2, etc., if existing.

~~2.11.25.1.3.~~2.11.24.1.3. For systems that support credit card payments – the PCI DSS standard is required.

~~2.11.25.1.4.~~2.11.24.1.4. For medical information systems – the HIPAA standard is required.

~~2.11.25.2.~~2.11.24.2. The bidder is to specify the work processes in the organization, and the tools used whose purpose is to ensure that Provider complies with all the rules and standards to which it is committed.

~~2.11.25.3.~~2.11.24.3. The bidder is to specify the levels of supervision, the levels of escalation for the handling of incidents, and the manner of dealing with unattended findings.

~~2.11.26.~~2.11.25. Segregation and compartmentalization of Clients

~~2.11.26.1.~~2.11.25.1. The Provider is to specify its capabilities, if any, to isolate and segregate a given Client, in relation to the following points:

~~2.11.26.1.1.~~2.11.25.1.1. Ability to prevent users of a certain Client from accessing another (different) Client's resources, unless such access has been permitted, even if the user has access authorizations to the other Client's resources. Prevention capabilities that are not based on the login system must be specified.

~~2.11.26.1.2.~~2.11.25.1.2. Ability to prevent different subscriber users from accessing subscriber resources, unless such access has been permitted, even if the other user has access authorizations to the subscriber's resources. The prevention capabilities that are not based on the login system must be specified.

~~2.11.26.1.3.~~2.11.25.1.3. Ability to create a specific address (IP or URI) for the Provider's services for a Client's users or a group of Clients, which is not shared with other Clients.

~~2.11.26.1.4.~~2.11.25.1.4. Receiving detailed logs showing access attempts that are inconsistent with the set rules.

Appendix 4.2 – requirements and questions regarding cyber protection, privacy and other issues in the field of information security for non-SaaS services

Serial no.	Name of the Service for witch the appendix is filled
1	
2	

(Rows may be added if necessary)

2.12. Directions on answering this appendix

2.12.1. In relation to each section, the bidder must confirm whether it meets the requirement set forth, and if required, state in the “answer details” column the manner in which the answer is implemented.

2.12.2. If the bidder does not meet the requirement in its entirety, it must specify the gaps in the “answer details” column.

2.12.3. It should be clarified that if the bidder saves or processes content data of Clients, or it can read, change, delete or perform any action on this data, including changing access authorization to it, the service will be considered to be SaaS.

#	Requirement	Bidder’s answer	Answer details
2.12.4. **Work configuration of the proposed service**			
2.12.4.1	Is the content data saved only on the Client's “network” (such as VPC)? If the information is not saved on the Client’s side, specify the location in which it is saved.	Yes / No	

2.12.4.2	If the content data processing is performed only on the client's "network" (such as VPC), if the content data is not processed on the Client's side, specify its processing location.	Yes / No	
2.12.4.3	Is the bidder unable to access the stored information or control the service or system? If it has access or control, specify the bidder's ability to access or control the information or system.	Yes / No	
2.12.4.4	Is all processing and access data saved on the Client's "network" without the bidder having access to it? If the bidder saves or has access to processing data, it must specify the location in which it is saved, its manner of protection against unauthorized access and the authorization process for viewing this data.	Yes / No	
2.12.4.5	If data is saved on the bidder's systems, does the bidder have an information deletion (Retention) policy? Specify this policy and the mechanisms it uses to delete the information when required.	Yes / No /Not applicable	
2.12.5. **Human capital security**			

2.12.5.1	Are there a review, verification and vetting processes done on the Provider's workers and those of its subcontractors, with attention to differences in processes according to the employee types and risk levels their function pose? Describe these processes, if any?	Yes / No	
2.12.5.2	Are there the initial and refresher training processes regards security, protection and cyber procedures for the employees of the Provider and subcontractors? Describe these processes, if any.	Yes / No	
2.12.5.3	Are there mechanisms for guarantee compliance with the procedures and the way of dealing with violations of security procedures or other critical procedures? Describe these processes, if any.	Yes / No	
2.12.5.4	Are tools used to detect human risks (such as detecting behavioral irregularities, feedback from supervisors or colleagues about problems, etc.) of functionaries in sensitive positions or with high access authorizations? Describe these processes, if any.	Yes / No	

2.12.6. Supply chain security

2.12.6.1	Are supply chain security processes and procedures in accordance with standards approved for the Provider by US Administration?	Yes / No	
2.12.6.2	Are supply chain security processes and procedures is in accordance with one of the following standards: NIST SP 800-53 Rev. 5/Nist SP 800-161 Rev. 1, or another international standard? Specify the standard.	Yes / No	
2.12.6.3	Is there an internal supply chain security standard? If there is, attach the internal standard as addendum.	Yes / No	
2.12.6.4	Are there review processes for introducing software from an external source and updates thereto, including checking for backdoors or planting of harmful abilities?	Yes / No	
2.12.6.5	Are there review processes for adding software from an internal source and updates thereto, including checking for backdoors or planting of harmful abilities?	Yes / No	

2.12.7. Configuration and change management security

2.12.7.1	Does the bidder follow an orderly configuration and change management policy for all systems participating in the provision of the services, in accordance with accepted and required standards? If so, specify the standard by which these processes are done, providing a schematic description of the configuration control system and the process of review, approval and documentation of changes.	Yes / No	
2.12.7.2	Does the development of the proposed systems managed by a Product Security Manager in accordance with orderly work procedures? If so, specify the main points of this work procedures	Yes / No	
2.12.8. **Support access**			
2.12.8.1	Does the bidder directly support the service (access to service / system operating on the Client's side)? If not, specify the supporting entity.	Yes / No	
2.12.8.2	Is there a process for supporter's access approval, which requires monitored, documented approval of the customer? Specify the approval track and the reviews applied to it.	Yes / No / Not applicable	

2.12.8.3	Are all access details, including unapproved access attempts, recorded in an orderly log including the details of the accessing party, details of the approver and any other relevant data?	Yes / No / Not applicable	
2.12.8.4	Is this log accessible to the Client?	Yes / No / Not applicable	
2.12.9. **Encryption and key management**			
2.12.9.1	Is it possible to set a default that requires content data encryption? If in to the judgment of the Provider, the encryption is not feasible, specify the reason for this.	Yes / No	
2.12.9.2	Does the service support encryption key management by the Client according to the Cloud Provider's abilities? Specify restrictions in this regard, if any.	Yes / No / Not applicable	
2.12.9.3	Would data encryption by proprietary systems of the Client impair provision of the service? Specify the implications of such encryption, if any.	Yes / No / Not applicable	
2.12.10. **Risk management**			

2.12.10	Does the bidder have an orderly risk management process in its organization? If it does, specify the standard by which the process is performed.	Yes / No	
2.12.10	The bidder to specify the security standard certificates held by the provider (as ISO 27001)	Yes / No	
2.12.11. **Login**			
2.12.11	Does the service fully interface with the IAM service of the Cloud Provider? Specify restrictions, if any?	Yes / No	
2.12.11	Does the service support one of the following login protocols: SAML, OpenID, OAuth for single Sign On with the Client's systems? Specify the supported protocols.	Yes / No / Not applicable	
2.12.12. **Logs**			
2.12.12	Does the service maintain logs in a standard configuration in the cloud provider's log systems? If not so, Specify the log process.	Yes / No	

Appendix 5 – Price Quotation

2.13. Guidelines for how to answer this appendix

2.13.1. The bidder must indicate a uniform discount for all the services it is offering in this Tender, according to the rules set forth in this appendix.

2.14. Provider's price quotation

Discount group name	**Minimum discount percentage**	**Offered discount percentage**
Discount for SaaS services	**Minimum discount from the overseas price list:** **20%**	**Discount from overseas price list:** **% ________________**
Discount for Non SaaS services	**Minimum discount from the overseas price list:** **30%**	**Discount from overseas price list:** **% ________________**
**** The discount percentage stated by the bidder will be greater than or equal to the minimum discount percentage **** **** The discount cannot be conditioned or restricted**** **** If a bidder did not submit a discount, his discount will be set as the minimum discount listed above ****		

2.15. Discount percentage

2.15.1. Subject to that specified in this section, the discount offered in the price quote will be valid for the entire duration of the agreement for all services that are being offered by the Provider under this Tender, In accordance with the groups above, including services that include human involvement (such as service that includes support) and future services in accordance with section 3.17 of the tender, and in all pricing methods which these services are offered in the Cloud Provider's services catalog (if offered using different pricing methods).

2.15.2. This discount will be in addition to the discounts built into the Provider's price list (such as a quantity discount, commitment based pricing etc.).

2.15.2.1. The Provider will be entitled to increase its discount during the engagement period. This change will be fixed from the time at which the new discount percentage is pronounced until the end of the engagement, except when the Provider asks to increase its discount again.

2.15.2.2. Without derogating from the aforesaid, the discount offered in each of the discount groups will be amended as follows during the engagement period:

2.15.2.2.1 Level A - when the volume of the combined usage of a certain service by all the Clients exceeds 1 million US$, during a calendar year, the percentage of the discount in each of the aforesaid groups will increase by 5 percentage points above that offered by the Provider in its offer (for example, if the offered discount for SaaS services is 25%, the new discount will be 30%).

2.15.2.2.2 Level B - when the volume of the combined usage of a certain service by all the Clients exceeds 5 million US$, during a calendar year, the percentage of the discount in each of the aforesaid groups will increase by 5 percentage points above the previous level.

2.15.2.3. If the discount changes in accordance with the levels specified above, and at the end of a calendar year the volume of purchases of a certain service, by all the clients, falls below the levels determined above, the Provider will be entitled to apply for the amendment of the discount back to the previous level of the discount, for the following calendar year.

2.16. Offered services price list

2.16.1. The price of the services for a Client under this tender will be determined according to the following mechanism:

2.16.1.1. The price of the services for the overseas region will be the price, as listed in the overseas price list of the service (as such term is defined below), as of the day of consumption of the services, minus the discount percentage offered by the Provider for that service.

2.16.1.2. The price of the services in the Israeli region will be the price, as listed in the overseas list price of the service, as of the day of consumption of the service, minus the discount percentage offered by the Provider for that service or the price, as listed in the list price of the service in the Israel region, as of the day of consumption of the service, minus the discount percentage offered by the Provider for that service, whichever is lower.

2.16.2. The overseas price list will be in accordance with one of the options specified below:

2.16.2.1. If the service is available in the service catalog in the overseas region:

2.16.2.1.1. The price list for the services offered in the digital marketplace of the Cloud Providers, as they appear in the overseas region.

2.16.2.1.2. The public price list of the service that is valid for customers in the overseas ~~area~~Region, if the service price list in the overseas ~~area~~Region refers to this price list.

2.16.2.2. If the service is not available in the service catalog in the overseas region: the public price list of the service manufacturer applicable in the country where the overseas region is located.

2.16.3. Below is an example of how to calculate the price of services:

2.16.3.1. If the overseas price list of the service is 1 US$ per hour of operation, and the discount offered is 35%, then the price of the service in the overseas ~~area~~Region will be 0.65 US$ per hour.

2.16.3.2. In this situation, if the list price of the service in the Israeli region is 1 US$ per hour or higher, the price of the service in the Israeli region will be 0.65 US$ per hour; however, if the price in the Israeli region is 0.8 US$ per hour, then the price of the service will be 0.52 US$ per hour (the lowest price of the service between the overseas region and the Israeli region will determine).

2.16.3.3. If the Provider increases the discount to 40%, this discount will apply to both the price list for the Israeli region and the price list for the overseas region, such that the overseas price list will be 0.6 US$ per hour, and the price of the service in the Israeli region will be 0.48 USD$ per hour.

2.16.4. Amendment of the overseas price list - in the event of a radical change in the price list of the services offered by the Provider in the digital marketplace in overseas region, as a result of exogenous changes that are not under the control of the Provider, and such do not exist in the Israeli region, the following arrangements will apply:

2.16.4.1. The Provider can contact the Tender Administrator with a request to change the overseas region to another region located in the European Union which is one of the 3 regions with the highest sales volume of the Cloud Provider in the European Union, with a justification for the request.

2.16.4.2. The Tender Administrator will examine the request positively and if the aforesaid request does not harm the Bidders in an unfair manner, will approve the request.

Appendix 6 - Manufacturer's statement

To:

Government Procurement Administration, Accountant General, Ministry of Finance

Subject: **Central Tender No. 01-2022 for the addition of services to the Government Digital Marketplace (hereinafter: the "Tender")**

2.17. I, the undersigned. _______________, hold the position of _____ _____________________ ___________________________ in _____________________ (hereinafter: the "**Manufacturer**"), which is the manufacturer of the following service(s) offered as part of the Tender (hereinafter: the "**Service**"):

Sequence no.	Name of the offered service for which this appendix has been submitted
1	
2	

(Rows may be added if necessary)

2.18. The service is offered in the tender by (mark **one** of the options):

□	Our company (the Manufacturer) or our subsidiary in Israel
□	~~Our~~Other company that is approved ~~distributor, and~~by the Manufacturer as the sole ~~offeror~~bidder of ~~our~~the services listed above ,as part of the Tender Specify the name of the ~~distributor~~Company _______________________(hereinafter: the "**Reseller**")

2.19. If the service is offered by the Manufacturer, it undertakes that it holds the full rights to sell the service offered in the Government Digital Marketplace in the tender, and to commit to the requirements of the tender.

2.20. If the service is offered by ~~a Distributor~~the Reseller, I declare and undertake as follows:

2.20.1. The ~~Distributor~~Reseller holds the full rights to offer the service in the tender, and to commit to the requirements of the tender for the service, including:

2.20.1.1. The terms of use of the service will be the terms of use specified in the tender. In the absence of an explicit or implicit provision in the provisions of the agreement or the tender, the standard and public service agreement of the provider which is used in the overseas region for customers of the size of the Israeli Government will apply.

2.20.1.2. The service will be operated in the Israeli ~~area~~Region in accordance with the provisions of section 3.6.3 of the tender documents, and in the accepted configuration of the service in other overseas regions where the service is deployed.

2.20.2. The response to Appendix 4 of the tender is made in a manner consistent with the characteristics of the service and the manner of its delivery by the Manufacturer.

2.20.3. The Manufacturer undertakes that whatever is required from the ~~Marketer~~Reseller plus the required assistance of the Manufacturer for the realization thereof, the Manufacturer will provide all the aforesaid assistance.

2.20.4. The Manufacturer will do everything ~~necessary for the Distributor~~demanded from him in regard to the operation of the service, in order for the Reseller to comply with the terms of the tender and the agreement thereunder, throughout the duration of the agreement.

Manufacturer name: ____

The role of the signatory of the Manufacturer: _____________________________

Date: ________________ Signature and stamp: ________________