REQUEST FOR PROPOSAL (RFP)

UNDP Albania Str. Skenderbej, Gurten Centre, 2nd floor, Tirana, Albania	DATE: December 22, 2021
	REFERENCE: Support and Maintenance for the Central Infrastructure of the Municipal OSSIS developed by STAR projects - "STAR3" Project ID: 00115505

Dear Sir / Madam:

We kindly request you to submit your Proposal for services **"Support and Maintenance for the Central Infrastructure of the Municipal OSSIS developed by STAR projects"**.

Please be guided by the form attached hereto as Annex 2, in preparing your Proposal. Proposals may be submitted on or before Monday, January 17, 2022 at 14:00 hrs via eTendering.

Allowable Manner of submitting proposals: **e-Tendering only. Bids not sent in e-Tendering system will not be considered**. Proposal Submission address: https://etendering.partneragencies.org

Please acknowledge receipt of this RFP by using the "Accept Invitation" function in e-tendering system. This will enable you to receive amendments or updates to the RFP. Please find the link for all procurement guides and videos:

https://www.undp.org/content/undp/en/home/procurement/business/resources-for-bidders.html

Electronic submission (e-Tendering) requirements:

- Format: PDF files only
- File names must be maximum 60 characters long and must not contain any letter or special character other than from Latin alphabet/keyboard.
- All files must be free of viruses and not corrupted.
- Max. File Size per transmission: 35 MB
- UNDP reserves the rights to ask for originals during the evaluation.

Please name the submitted files following the structure and the solicitation document and consolidate the files into as few files as possible, using compression tools (ZIP etc.).

Your Proposal must be expressed in the English Language, and valid for a minimum period of 120 (one hundred and twenty) days.

In the course of preparing your Proposal, it shall remain your responsibility to ensure that it reaches the address above on or before the deadline. Proposals that are received by UNDP after the deadline indicated above, for whatever reason, shall not be considered for evaluation. Services proposed shall be reviewed and evaluated based on completeness and compliance of the proposal and responsiveness with the requirements of RFP and all other annexes providing details of UNDP requirements.

The Proposal that complies with all of the requirements, meets all the evaluation criteria and offers the best value for money shall be selected and awarded the contract. Any offer that does not meet the requirements shall be rejected.

Any discrepancy between the unit price and the total price shall be re-computed by UNDP, and the unit price shall prevail, and the total price shall be corrected. If the Contractor does not accept the final price based on UNDP's re-computation and correction of errors, its Proposal will be rejected.

No price variation due to escalation, inflation, fluctuation in exchange rates, or any other market factors shall be accepted by UNDP after it has received the Proposal. At the time of Award of Contract or Purchase Order, UNDP reserves the right to vary (increase or decrease) the quantity of services and/or goods, by up to a maximum twenty-five per cent (25%) of the total offer, without any change in the unit price or other terms and conditions.

Any Contract or Purchase Order that will be issued as a result of this RFP shall be subject to the General Terms and Conditions attached hereto. The mere act of submission of a Proposal implies that the Contractor accepts without question the General Terms and Conditions of UNDP, herein attached as Annex 3.

Please be advised that UNDP is not bound to accept any Proposal, nor award a contract or Purchase Order, nor be responsible for any costs associated with a Contractors preparation and submission of a Proposal, regardless of the outcome or the manner of conducting the selection process.

UNDP's vendor protest procedure is intended to afford an opportunity to appeal for persons or firms not awarded a Purchase Order or Contract in a competitive procurement process. In the event that you believe you have not been fairly treated, you can find detailed information about vendor protest procedures in the following link:

http://www.undp.org/content/undp/en/home/operations/procurement/business/protest-and-sanctions.html

UNDP encourages every prospective Contractor to prevent and avoid conflicts of interest, by disclosing to UNDP if you, or any of your affiliates or personnel, were involved in the preparation of the requirements, design, cost estimates, and other information used in this RFP.

UNDP implements a zero tolerance on fraud and other proscribed practices, and is committed to preventing, identifying and addressing all such acts and practices against UNDP, as well as third parties involved in UNDP activities. UNDP expects its Contractors to adhere to the UN Supplier Code of Conduct found in this link :

https://www.un.org/Depts/ptd/sites/www.un.org.Depts.ptd/files/files/attachment/page/pdf/unscc/conduct_english.pdf

Thank you and we look forward to receiving your Proposal.

Sincerely yours,

Monica Merino
Resident Representative

Annex 1

Description of Requirements

Context of the Requirement	In partnership with the Government of Albania and supported by the European Union, Sweden, and Switzerland, UNDP Albania is implementing the project 'STAR3 – Sustaining and Advancing Local Governance Reform'. STAR3 is implemented in the context of the post Territorial and Administrative Reform, following its two predecessors, STAR1 and STAR2, and built upon their results and the evolving context. As a cumulative result of STAR2 and STAR3 efforts, during the period 2018-2020, OSSIS has been already rolled out in the central offices of 50 municipalities of Albania. STAR3 is committed to take the challenge further by expanding OSS to the level of Administrative Units, as a crucial move to address the rural-urban divide and provide equal opportunities and ease of access for all citizens of Albania despite their location. OSSIS operates from a central IT infrastructure hosted on the e-Government infrastructure (NAIS Datacenter) where End-User is the General Directorate Local Administration. The system is being used by the central municipalities' front-office and back-office employees in the process of public administrative services provision to the citizens and businesses. More than 70 services are configured in each LGU OSSIS, categorized in 11 categories based on a mapping of the business processes in the target municipalities. The list of configured services will be increased as well, allowing for additional ones if needed. During 2022 STAR3 is planning to enhance of OSSIS usage and its rollout to more than 250 AU. Such planned increase of OSSIS usage will bring increased traffic load to the underlying central IT infrastructure. The OSSIS central infrastructure has been installed and made operational during STAR2 since November 27, 2018 on the GoA Data Centre which is operated by the National Agency for Information Society (NAIS). The hardware delivered (HPE, FORTINET and KEMP) is fully operational, but currently with expired original manufacturer's warranty and without support and maintenance services. The scope of this contract is to ensure maintenance and support services for the central OSSIS IT infrastructure for a period until December 31st, 2023. During the contract validity, the service provider should collaborate closely with NAIS for coordinating visits on the premises as needed and collaborate as well with the service provider in charge of municipal OSSIS support and AU rollout. Below are presented the details of central hardware solution supporting OSS system functionality subject to the required maintenance and support service in these ToRs including:

	1. Server and Storage infrastructure 2. Network Infrastructure 3. Licensing, and 4. Detailed list of hardware components
Implementing Partner of UNDP	Ministry of Interior (MoI), National Agency for Information Society (NAIS)
Brief Description of the Required Services[1]	To ensure proper and uninterrupted operation of the OSSIS central IT infrastructure, the following requirements describe the terms and conditions for acceptable maintenance and support services to be contracted. 4.1 Coverage Period. Support will start on February 01, 2022 and will be in place until December 31, 2023. 4.2 Maintenance Support services required. The Bidder should offer and deliver official Service from vendors (Microsoft, HPE, Fortinet and Kemp) for the time period required. Vendor support for the first year will be activated with starting date February 01, 2022 with 23 months validity. The activation of the support for the first year should include any "return to support" or "support change" in line with the vendors' policy of support. Official service from vendors (Microsoft, HPE, Fortinet and Kemp) is required to ensure: (i) case logging and handling (for both hardware and software); (ii) vendor resolution of support cases including approved task list for any intervention; (iii) escalation procedures to facilitate the resolution of complex *incidents; (iv) free of charge supply of genuine spare part to replace defective ones; (v) software update (patches, fixes, new versions allowed) if any during the coverage period of support. The Bidder should also ensure: (i) Single Point of Contact (SPOC) for handling cases; (ii) on-site support through trained and qualified engineers; (iii) periodic (quarterly) systems health checks; (iv) logistics for any necessary spare parts and media required. *Note: Incident or Support Case is a technical problem affecting normal operation of equipment.* In more detail, the Awarded Bidder should implement the following tasks: 4.2.1 Preliminary evaluation.

[1] *A detailed TOR may be attached if the information listed in this Annex is not sufficient to fully describe the nature of the work and other details of the requirements.*

Within one week of contract signing, service provider should make a preliminary evaluation of the status for all the equipment, that will include (i) health check of all equipment part of central IT infrastructure; (ii) collect logs of all equipment; (iii) check status of applied patches and fixes recommended by the vendors. Based on this evaluation, service provider will prepare a report with the findings and the actions to be taken for the proper operation of all equipment. Part of the proposal should be included the methodology and a check list with approximate scheduling.

4.2.2 Periodic checks.
Service provider apart of almost real time monitoring should perform periodically health checks during which will complete the following activities: (i) physical check of equipment; (ii) collection of logs from equipment; (iii) application of any patch, fix recommended by vendors; (iv) install critical firmware updates recommended by vendors for immediate installation.

Periodic checks will be done within the last week of each quarter and service provider will provide the End-User with a document with findings, logs and all activities performed. The quarterly document will also include the ticket records of all support cases opened during the quarter and their statuses.

4.2.3 Case logging and incident resolution.
Service provider and vendors acknowledge a support incident by logging a support case, communicating the case ID to the End-User, and confirming the incident severity and time requirements for commencement of remedial action. Each case will be recorded and each step till the resolution of the incident will be documented.

4.2.4 Remote problem diagnosis and support.
Once the end-user has placed a call and it has been acknowledged, service provider and vendors should work to isolate the incident and to remotely troubleshoot, remedy, and resolve the incident with the End-User. Prior to any on-site assistance, service provider may initiate and perform remote diagnostics using electronic remote support solution to access covered products or may use other means available to facilitate remote incident resolution. Based on the problem diagnoses and remote assistance the incident may be resolved or may require further actions.

4.2.5 On-site hardware support.
For hardware incidents that cannot be resolved remotely, service provider assigns an authorized representative to provide on-site technical support on covered hardware products to return them to operating condition. Once the technical personnel arrive at the NAIS site, it may continue troubleshooting until the problem related to the central IT infrastructure is resolved or successfully diagnosed and the necessary steps to its resolutions are priory agreed with the end-user.

In addition, at the time of on-site technical support delivery, service provider may: (i) install available engineering improvements for covered hardware products to help ensure proper operation of the hardware products and maintain compatibility with supplied hardware replacement parts; (ii) install available firmware updates defined by vendor that are required to return the covered product to operating condition or to maintain supportability.

End-User and service provider should strictly follow all measures in place by the Government of Albania against spread of Covid-19 virus. It is under the service provider's responsibility to ensure that the authorized representative is fully instructed and follows the measures during any interventions in performing on-site support activities based on NAIS regulations.

4.2.6 Replacement parts and materials.
Contractor and vendors provide free of charge genuine replacement parts and materials necessary to maintain the covered hardware product in operating condition, including parts and materials for available engineering improvements required by vendors to assure supportability of the product.

Replacement parts provided under hardware support will be unit replacements or new or functionally equivalent to new in performance and reliability and warranted as new. Replaced (defective) parts will be returned to their corresponding vendor.

All equipment installed have been configured with redundant hardware options on all critical components such as power supplies, controllers, hard disc drives, memories, etc. as well as on logical configuration such as redundant roles RAID protection and continuous backup and restore. However, ensuring fast defective part replacement is crucial in maintaining the central site in normal operation.

4.2.7 Software Support.
The equipment listed in Section 3 does have software installed. For software products covered by the required support service, service provider and vendors have to provide corrective support to resolve identifiable software product problems, support to help identify problems and provide assistance in troubleshooting problems and determining configuration parameters for supported configurations.

Software support will include the license-to-use software updates from their manufactures. Part of the support delivery should be recommended software update method and recommended documentation on upgrade method.

For networking and security products, service provider and vendor have to provide real-time threat intelligence updates to block and prevent advanced cyber threats.

Service provider has to provide information, as commercially available by vendors, on current product features, known problems and available solutions, and operational advice and assistance.

4.2.8 Incident severity levels.

- ✓ Severity 1 -critical business impact: For example, production environment down: production system or production application down/critically impacted; data corruption/loss or risk; business continuity severely affected; safety and security issues.
- ✓ Severity 2 -limited business impact or business risk: For example, production environment available but some functions limited or degraded; severely restricted use; critical nonproduction environment or system issue.
- ✓ Severity 3 -no business impact: For example, nonproduction system (such as test system) or noncritical issue; work around in place, installations, questions, or requests for information or guidance.

SLAs for incident's resolution as per severity levels are defined as follows:

Feature Required	**Severity 1**	**Severity 2**	**Severity 3**
Access for case logging	24 x 7, Every day, holidays included		
Case logging Window	24 x 7, Every day, holidays included	24 x 7, Every day, holidays included	8:00 a.m. and 5:00 p.m., business days
Case logging requirements	Detailed Incident Description on the affected equipment		
Phone Response (remote)	Remote response 24x7 15m call back	Remote response 24x7 2-hour call back call back	Remote response, Next-Business-Day call back
E-mail Response (remote)	24 x 7, Every day, holidays included	24 x 7, Every day, holidays included	8:00 a.m. and 5:00 p.m., business days
On-site response (Hardware)	within 4-hour on-site	4-hour on-site	Next-Business-Day on-site
Parts replacement	Best effort by service provider and vendor. Should not compromise operation		
Parts replacement window	24 x 7, Every day, holidays included		Next-Business-Day
Software support	24 x 7, Every day, holidays included		Next-Business-Day
Automated incident logging	Should be available through installation of vendor's proprietary service tools		

Repair is considered complete upon the verification that the hardware malfunction has been corrected or that the hardware has been replaced.

4.2.9 Accepted Support Service limitations.
Activities such as, but not limited to, the following are excluded from the support:

- Unauthorized attempts by third-party personnel to install, repair, maintain, or modify hardware, firmware, or software;

	- Services required due to improper treatment or use of the products or equipment; - Non-designated usage of hardware or software, or usage thereof in contradiction with the recommendations from the vendors; - Troubleshooting for interconnectivity or compatibility problems; 4.2.10 Communication between parties. All communication by the parties should be recorded and documented accordingly. Only authorized representatives should have access on the communications. For this purpose, End-User and service provider assign authorized representatives identified with name, surname, position within organization, telephone number, e-mail address and office address. E-mail address and Call Center telephone numbers of the vendors for the support purposes should be available for both parties. 4.2.11 Real time monitoring All equipment's should be monitoring in real time events and categorized based on its severity. Automatic rules should be defined to send alerts accordingly. The service provide should propose accordingly how exactly will be performed such activity, tools to be used, what will be monitored, personnel that will be in charge of configuration/ monitoring and important rules to be described how they will be configured.
List and Description of Expected Outputs to be Delivered	23 months support and maintenance for Central IT Infrastructure of Municipal OSSIS. Reports: - Submission of 1st Quarterly Report for 2022 as per the Maintenance and Support requirements. – End of March 2022 - Submission of 2nd Quarterly Report for 2022 as per the Maintenance and Support requirements. – End of June 2022 - Submission of 3rd Quarterly Report for 2022 as per the Maintenance and Support requirements. – End of September 2022 - Submission of 4th Quarterly Report for 2022 as per the Maintenance and Support requirements. – End of December 2022 - Submission of 1st Quarterly Report for 2023 as per the Maintenance and Support requirements. – End of March 2023 - Submission of 2nd Quarterly Report for 2023 as per the Maintenance and Support requirements. – End of June 2023 - Submission of 3rd Quarterly Report for 2023 as per the Maintenance and Support requirements. – End of September 2023 - Submission of 4th Quarterly Report for 2023 as per the Maintenance and Support requirements. – End of December 2023 - Handover document to government counterparts – End of December 2023

Person to Supervise the Work/Performance of the Contractor	The Contractor will work under the overall supervision of UNDP Albania /STAR3, to which the Contractor will directly report, seek approval, and obtain the acceptance of deliverables. Upon the completion of work assignments, the supervisor will evaluate the consultant's work, certify relevant documents and process/follow-up on the payments.
Frequency of Reporting	The Contractor will submit Quarterly Reports on the Support services provided. Moreover, monthly meetings will take place in case of potential issues evidenced.
Progress Reporting Requirements	Written Communication
Location of work	National Agency for Information Society (NAIS) premises in Tirana, Albania including remote and on-site support.
Expected duration of work	23 Months
Target start date	1 February 2022
Latest completion date	31 December 2023
Travels Expected	N/A
Special Security Requirements	N/A
Facilities to be Provided by UNDP (i.e., must be excluded from Price Proposal)	N/A
Implementation Schedule indicating breakdown and timing of activities/sub-activities	☒ Required ☐ Not Required
Names and curriculum vitae of individuals who will be involved in completing the services	☒ Required ☐ Not Required
Currency of Proposal	☐ United States Dollars ☐ Euro ☒ Local Currency

<table>
<tr><td>Value Added Tax on Price Proposal[2]</td><td>☒ must be inclusive of VAT and other applicable indirect taxes
<b>Re VAT, offerors should clearly indicate: 1) whether they are subject of VAT payment and 2) whether the applicable VAT for the present submission is 0.</b>

☐ must be exclusive of VAT and other applicable indirect taxes</td></tr>
<tr><td>Validity Period of Proposals <i>(Counting for the last day of submission of quotes)</i></td><td>☐ 60 days
☐ 90 days
☒ 120 days

In exceptional circumstances, UNDP may request the Proposer to extend the validity of the Proposal beyond what has been initially indicated in this RFP. The Proposal shall then confirm the extension in writing, without any modification whatsoever on the Proposal.</td></tr>
<tr><td>Partial Quotes</td><td>☒ Not permitted
☐ Permitted</td></tr>
<tr><td>Payment Terms[3]</td><td>UNDP shall affect payments to the Contractor after acceptance by UNDP of the deliverables (with a prior clearance from the STAR3), submission of the corresponding invoices submitted by the Contractor, and in accordance with the following schedule of payments corresponding to the achievement of the indicated milestones and deliverables (please refer to the ToRs for details).
<table>
<tr><th>Instalments</th><th>Quantity</th><th>Conditions</th></tr>
<tr><td>1st installment</td><td>20%</td><td>▪ After submission of 1st and 2nd Quarterly Reports (2022) as per the Maintenance and Support requirements
05 Jul 2022</td></tr>
<tr><td>2nd installment</td><td>30%</td><td>▪ After submission of 3rd and 4th Quarterly Reports (2022) as per the Maintenance and Support requirements
20 Dec 2022</td></tr>
<tr><td>3rd installment</td><td>50%</td><td>▪ After submission of 1st, 2nd, 3rd, and 4th Quarterly Reports (2023) as per the Maintenance and Support requirements, and
▪ Handover document to government counterparts
20 Dec 2023</td></tr>
</table></td></tr>
<tr><td>Person(s) to review/inspect/ approve outputs/complete</td><td>STAR3 Project Manager, STAR3 OSSIS Expert, and Programme Specialist</td></tr>
</table>

[2] *VAT exemption status varies from one country to another. Pls. check whatever is applicable to the UNDP CO/BU requiring the service.*

[3] *UNDP preference is not to pay any amount in advance upon signing of contract. If the Contractor strictly requires payment in advance, it will be limited only up to 20% of the total price quoted. For any higher percentage, or any amount advanced exceeding $30,000, UNDP shall require the Contractor to submit a bank guarantee or bank cheque payable to UNDP, in the same amount as the payment advanced by UNDP to the Contractor.*

d services and authorize the disbursement of payment	
Type of Contract to be Signed	☐ Purchase Order ☐ Institutional Contract ☒ Contract for Professional Services ☐ Long-Term Agreement[4] ☐ Other Type of Contract
Criteria for Contract Award	☐ Lowest Price Quote among technically responsive offers ☒ Highest Combined Score (based on the 70% technical offer and 30% price weight distribution) ☒ Full acceptance of the UNDP Contract General Terms and Conditions (GTC). This is a mandatory criterion and cannot be deleted regardless of the nature of services required. Non-acceptance of the GTC may be grounds for the rejection of the Proposal.
Criteria for the Assessment of Proposal	**Technical Proposal (70%)** ☒ Expertise of the Firm 30% ☒ Methodology, Its Appropriateness to the Condition and Timeliness of the Implementation Plan 40% ☒ Management Structure and Qualification of Key Personnel 30% **Financial Proposal (30%)** To be computed as a ratio of the Proposal's offer to the lowest price among the proposals received by UNDP.
UNDP will award the contract to:	☒ One and only one Contractor ☐ One or more Contractors, depending on the following factors:
Contract General Terms and Conditions[5]	☒ General Terms and Conditions for contracts (goods and/or services) ☐ General Terms and Conditions for de minimis contracts (services only, less than $50,000) Applicable Terms and Conditions are available at: http://www.undp.org/content/undp/en/home/procurement/business/how-we-buy.html
Annexes to this RFP[6]	☒ Form for Submission of Proposal (Annex 2) ☒ Detailed TOR ☐ Others[7]

[4] *Minimum of one (1) year period and may be extended up to a maximum of three (3) years subject to satisfactory performance evaluation. This RFP may be used for LTAs if the annual purchases will not exceed $200,000.00.*

[5] *Contractors are alerted that non-acceptance of the terms of the General Terms and Conditions (GTC) may be grounds for disqualification from this procurement process.*

[6] *Where the information is available in the web, a URL for the information may simply be provided.*

[7] *A more detailed Terms of Reference in addition to the contents of this RFP may be attached hereto.*

Contact Person for Inquiries (Written inquiries only)[8]	*UNDP Albania Procurement Unit* Any delay in UNDP's response shall be not used as a reason for extending the deadline for submission, unless UNDP determines that such an extension is necessary and communicates a new deadline to the Proposers.
Other Information *[pls. specify]*	N/A

[8] *This contact person and address is officially designated by UNDP. If inquiries are sent to other person/s or address/es, even if they are UNDP staff, UNDP shall have no obligation to respond nor can UNDP confirm that the query was received.*

Annex 2

FORM FOR SUBMITTING CONTRACTOR'S PROPOSAL[9]

(This Form must be submitted only using the Contractor's Official Letterhead/Stationery[10])

[insert: *Location]*.
[insert: *Date]*

To: *[insert: Name and Address of UNDP focal point]*

Dear Sir/Madam:

We, the undersigned, hereby offer to render the following services to UNDP in conformity with the requirements defined in the RFP dated *[specify date]* , and all of its attachments, as well as the provisions of the UNDP General Contract Terms and Conditions :

A. Qualifications of the Contractor

The Contractor must describe and explain how and why they are the best entity that can deliver the requirements of UNDP by indicating the following :

a) Profile – describing the nature of business, field of expertise, licenses, certifications, accreditations;
b) Business Licenses – Registration Papers, Tax Payment Certification, etc.
c) Latest Audited Financial Statement – income statement and balance sheet to indicate Its financial stability, liquidity, credit standing, and market reputation, etc. ;
d) Track Record – list of clients for similar services as those required by UNDP, indicating description of contract scope, contract duration, contract value, contact references;
e) Certificates and Accreditation – including Quality Certificates, Patent Registrations, Environmental Sustainability Certificates, etc.
f) Written Self-Declaration that the company is not in the UN Security Council 1267/1989 List, UN Procurement Division List or Other UN Ineligibility List.

B. Proposed Methodology for the Completion of Services

The Contractor must describe how it will address/deliver the demands of the RFP; providing a detailed description of the essential performance characteristics, reporting conditions and quality assurance mechanisms that will be put in place, while demonstrating that the proposed methodology will be appropriate to the local conditions and context of the work.

[9] *This serves as a guide to the Contractor in preparing the Proposal.*

[10] *Official Letterhead/Stationery must indicate contact details – addresses, email, phone and fax numbers – for verification purposes*

C. Qualifications of Key Personnel

If required by the RFP, the Contractor must provide:

a) Names and qualifications of the key personnel that will perform the services indicating who is Team Leader, who are supporting, etc.;
b) CVs demonstrating qualifications must be submitted if required by the RFP; and
c) Written confirmation from each personnel that they are available for the entire duration of the contract.

D. Cost Breakdown per Deliverable*

	Deliverables ***[list them as referred to in the RFP]***	**Percentage of Total Price** ***(Weight for payment)***	**Price** ***(Lump Sum, All Inclusive)***
1	Deliverable 1		
2	Deliverable 2		
3	....		
	Total	100%	

**This shall be the basis of the payment tranches*

E. Cost Breakdown by Cost Component *[This is only an Example]*:

Description of Activity	**Remuneration per Unit of Time**	**Total Period of Engagement**	**No. of Personnel**	**Total Rate**
I. Personnel Services				
1. Services from Home Office				
a. Expertise 1				
b. Expertise 2				
2. Services from Field Offices				
a . Expertise 1				
b. Expertise 2				
3. Services from Overseas				
a. Expertise 1				
b. Expertise 2				
II. Out of Pocket Expenses				
1. Travel Costs				
2. Daily Allowance				
3. Communications				
4. Reproduction				
5. Equipment Lease				
6. Others				
III. Other Related Costs				

[Name and Signature of the Contractor's Authorized Person]
[Designation]
[Date]

Annex 3

Terms of Reference (ToR)

Support and Maintenance for the Central Infrastructure of the Municipal OSSIS developed by STAR projects

1. Background

In partnership with the Government of Albania and supported by the European Union, Sweden, and Switzerland, UNDP Albania is implementing the project 'STAR3 – Sustaining and Advancing Local Governance Reform'.

STAR3 is implemented in the context of the post Territorial and Administrative Reform, following its two predecessors, STAR1 and STAR2, and built upon their results and the evolving context.

As a cumulative result of STAR2 and STAR3 efforts, during the period 2018-2020, OSSIS has been already rolled out in the central offices of 50 municipalities of Albania. STAR3 is committed to take the challenge further by expanding OSS to the level of Administrative Units, as a crucial move to address the rural-urban divide and provide equal opportunities and ease of access for all citizens of Albania despite their location.

OSSIS operates from a central IT infrastructure hosted on the e-Government infrastructure (NAIS Datacenter) where End-User is the General Directorate Local Administration.

The system is being used by the central municipalities' front-office and back-office employees in the process of public administrative services provision to the citizens and businesses. More than 70 services are configured in each LGU OSSIS, categorized in 11 categories based on a mapping of the business processes in the target municipalities. The list of configured services will be increased as well, allowing for additional ones if needed. During 2022 STAR3 is planning to enhance of OSSIS usage and its rollout to more than 250 AU. Such planned increase of OSSIS usage will bring increased traffic load to the underlaying central IT infrastructure.

2. Scope of services

The OSSIS central infrastructure has been installed and made operational during STAR2 since November 27, 2018 on the GoA Data Centre which is operated by the National Agency for Information Society (NAIS).

The hardware delivered (HPE, FORTINET and KEMP) is fully operational, but currently with expired original manufacturer's warranty and without support and maintenance services.

The scope of this contract is to ensure maintenance and support services for the central OSSIS IT infrastructure for a period until December 31st, 2023.

During the contract validity, the service provider should collaborate closely with NAIS for coordinating visits on the premises as needed and collaborate as well with the service provider in charge of municipal OSSIS support and AU rollout.

Below are presented the details of central hardware solution supporting OSS system functionality subject to the required maintenance and support service in these ToRs including:

a. Server and Storage infrastructure

b. Network Infrastructure

c. Licensing, and

d. Detailed list of hardware components.

3. Description of the Solution

The central IT infrastructure solution is used to host the One Stop Shop Information System (OSSIS) and to address all the functional requirements for having a high available, scalable, and fault-tolerant solution.

The OSSIS system runs in three environments (Training, Test and Production). Training and Production environment are hosted in Central (NAIS) Datacenter located in Tirana and the Test environment is configured on service provider own hardware, where three virtual machines in the roles of Web, Application and Database are configured.

The infrastructure is based on virtualization of hardware resources for the application layer and middleware, while the database layer is not virtualized.

The roles created on the IT central infrastructure are described below:

3.1 Server & Storage Infrastructure

Server & Storage components are used to create the following services.

Active Directory Service

Active Directory's OUs are created based on the infrastructure hierarchy and domain controller policies are secured with well configured GPOs as per Microsoft best practices.

Microsoft Hyper-V Failover Cluster

Hyper-V Failover Cluster is created with 3 physical servers which have the same hardware and software specifications. All nodes are physically connected to the dedicated storage and use the same CSV storage location for storing VMs running on cluster. Failover Cluster has configured 3 virtual network adapters for different services such as Live Migration, Heartbeat and for Management of OS. Live Migration virtual network adapter is used for migration of VMs from one node to another node. Heartbeat virtual network adapter determines the communication of the cluster nodes whether a node is up and running for hosting the system workloads.

Management of OS virtual network adapter provides connectivity between OS and physical Hyper-V host and is used for management of the server that is running Hyper-V and VMs. The physical servers have Microsoft Windows Server 2016 Datacenter Edition in order to provide unlimited number of virtual machines.

Microsoft SQL Server Always ON Availability

Database layer has two redundant servers who are directly connected to storage STO_DB01 and STO_DB02 respectively. SQL Always ON Availability group is available on both servers for high availability and real-time replication of hosted databases between both DB servers. Licensing of this infrastructure uses Windows 2016 Standard Operating System as well as SQL 2016 Enterprise Edition license.

Application and Web Server

The solution for the application and web server dedicated infrastructure consists of 3 virtual machines for each service, built over three physical nodes in Hyper-V Failover Clustering. Application and web servers have IIS role and Network Load Balancing feature installed and configured. Operating system of the application and web servers is Windows Server 2016 Standard.

Monitoring solution

A virtual SCOM server is created for infrastructure monitoring purpose. All Infrastructure components of hardware and software are monitored by the Microsoft System Center Operation Manager 2016. Each service is being monitored by configuring the respective Management Pack of both Windows and Hardware Vendor Management. This solution makes possible to generate a detailed availability and performance reports of the infrastructure as well as monitor and solve active infrastructure alerts, warnings and errors in real time.

Backup Server Solution

A dedicated physical server for backing up all data of the infrastructure is configured. This Server has installed Windows Server 2016 Standard operating system, Microsoft System Center Data Protection Manager 2016 and SQL Server 2016 Standard. This server has internal attached RAID5 disk layout and a tape library attached for storing the backups of infrastructure. Backup schedules and retention ranges are configured based on the sensitivity of the system. Backups are scheduled both for disk and tape backups.

Reporting Server

This server is configured in a dedicated hyper-v failover cluster. This cluster shares a dedicated partition from storage from STO_VM_00. NODE_A and NODE_B are physical nodes of hyper-v failover cluster for reporting services.

In order to enhance the data analytic capabilities during the first year of STAR3, Power BI on O365 is being implemented separately. The Reporting Server serves as well as a data warehouse and data source for Power BI.

DIS Server

A physical DIS server is installed and two virtual machines are configured. This server serves for the integration of the system with the GG platform. Licensing used is Windows Server 2016 Standard as well as SQL Server Standard and BizTalk Licenses for each of the virtual machines configured in the virtual environment.

ADFS Server

A dedicated virtual server for ADFS services is created on Hyper-V Cluster with the purpose to provide federation to other forest domains and single sign-on access to systems and applications located across organizational boundaries.

3.2 Network Infrastructure

Network Infrastructure components include:

Core Switches (2 x HPE 5130 24G 4SPF + EI Switch)

Two switches are used for this infrastructure in the role of core switches. They are configured in a stack using 10GE ports to ensure redundancy and reliability. Since these switches offer interconnection for all network and system devices, they also provide high performance and throughput too. Core switches are configured with L3 function in order to enable traffic routing between internal systems and the outside infrastructure.

Edge Firewall solution (2 x FORTINET FortiGate 201E)

In order to ensure redundancy and high availability, a cluster of two firewalls is configured. This cluster of Edge Firewall provides the security perimeter to protect internal systems, interconnect with Government Gateway infrastructure and access to Internet. Secure communication is applied to terminate IPsec site to site VPN tunnel from remote sites. Public IP addresses are assigned to outer interface in order to provide reachability by remote site from different service provider. Dedicated interfaces are used for outside, inside segments and cluster communication. Communication with outside and inside infrastructure will be done with dynamic routing and static routing. Firewalls also have included IPS services.

Edge Firewalls provide high throughput and performance due to the nature of services offered by this infrastructure.

Hardware Load Balancer (2 x KEMP LoadMaster LM-X15 Load Balancer)

A cluster of two hardware load balancers is being used to provide load share between web servers and application servers too. They are configured in a high availability cluster. High throughput and performance are also applied to offer best performance and low latency during service access. Load balancers are configured to publish only specific service for internal server.

3.3 Licensing

The infrastructure described has the following licenses from Microsoft vendor:

DIS Server license	**Qty**
SysCtrStdCore LicSAPk OLP 16cores	1
WinSvrSTDCore 2016 OLP 16cores	2
BztlkSvrStd 2016 OLP 4cores	2
SQLSvrStd 2016 OLP	2

Servers Cluster license	**Qty**
WinSvrDCCore 2016 OLP 20cores	3
SysCtrDatactrCore LicSAPk OLP 20cores	3

DPM+DC license	**Qty**
WinSvrSTDCore 2016 OLP 16core	2
SysCtrStdCore LicSAPk OLP 16cores	1

Database server license	Qty
WinSvrSTDCore 2016 OLP 40 core	2
SQLSvrEntCore LicSAPk OLP 2 cores	8
SysCtrStdCore LicSAPk OLP 40 cores	2

Reporting servers license	Qty
WinSvrSTDCore 2016 OLP 16core	2
SysCtrStdCore LicSAPk OLP 16cores	2
SQLSvrEntCore LicSAPk OLP 2cores	4
0365 Power BI Pro / Per user	4
0365 Power BI Premium / Per user	1

3.4 List of components

Nr.	Component	Product Description	Vendor	Serial Number
1.1.	Switch	HPE 5130 24G 4SPF + EI Switch	HPE	CN84GPV0L5
1.2.	Switch	HPE 5130 24G 4SPF + EI Switch	HPE	CN84GPV0LB
2.1.	Firewall	FORTINET FortiGate 201E	FORTINET	FG201ETK18903125
2.2.	Firewall	FORTINET FortiGate 201E	FORTINET	FG201ETK18903138
3.1.	Loadbalancer	KEMP LoadMaster LM-X15 Load Balancer	KEMP	TSBI03017751
3.2.	Loadbalancer	KEMP LoadMaster LM-X15 Load Balancer	KEMP	TSBI03017753
4.1.	Blade Enclosure	HPE BladeSystems BLc7000 Enclosure	HPE	CZ3833B1W4
5.1.	Server Blade 1 - DB	HPE BL660c G9 Blade	HPE	CZ283401V9
5.2.	Server Blade 1 - DB	HPE BL660c G9 Blade	HPE	CZ283401VB
6.1.	Server Blade 2 - HV Node	HPE Blade Servers BL460c G9	HPE	CZ28330DVJ
6.2.	Server Blade 2 - HV Node	HPE Blade Servers BL460c G9	HPE	CZ28330DVH
6.3.	Server Blade 2 - HV Node	HPE Blade Servers BL460c G9	HPE	CZ28330DVG
7.1.	Server Blade 3 - SCOM/File server	HPE Blade Servers BL460c G9	HPE	CZ28330DVK
8.1.	Server Blade 4 - AD	HPE Blade Servers BL460c G9	HPE	CZ28330DVL
9.1.	Server Blade 5 - Reporting Node	HPE Blade Servers BL460c G9	HPE	CZ28330DVN
9.2.	Server Blade 5 - Reporting Node	HPE Blade Servers BL460c G9	HPE	CZ28330DVM
10.1.	Server Rack Mount - DIS	HPE DL360 G9	HPE	CZ38329TJC
11.1.	Storage Array (Storage Box) - SAN Storage for HV Servers	HPE 3PAR 8200	HPE	CZ3833B01C
12.1.	Storage Array (Storage Box) - SAN Storage for DB Servers	HPE 3PAR 8200	HPE	CZ3833B01G

12.2.	Storage Array (Storage Box) - SAN Storage for DB Servers	HPE 3PAR 8200	HPE	CZ3833B01F
13.1.	Tape Library	HPE MSL2024	HPE	DEC83306EP

4. Description of the Maintenance and Support Service required.

To ensure proper and uninterrupted operation of the OSSIS central IT infrastructure, the following requirements describe the terms and conditions for acceptable maintenance and support services to be contracted.

4.1 Coverage Period.

Support will start on February 01, 2022 and will be in place for two consecutive years till December 31, 2023.

4.2 Maintenance Support services required.

The Bidder should offer and deliver official Service from vendors (Microsoft, HPE, Fortinet and Kemp) for the time period required. Vendor support for the first year will be activated with starting date February 01, 2022 with 23 months validity. The activation of the support for the first year should include any "return to support" or "support change" in line with the vendors' policy of support.

Official service from vendors (Microsoft, HPE, Fortinet and Kemp) is required to ensure:
(i) case logging and handling (for both hardware and software);
(ii) vendor resolution of support cases including approved task list for any intervention;
(iii) escalation procedures to facilitate the resolution of complex *incidents;
(iv) free of charge supply of genuine spare part to replace defective ones;
(v) software update (patches, fixes, new versions allowed) if any during the coverage period of support.

The Bidder should also ensure:
(i) Single Point of Contact (SPOC) for handling cases;
(ii) on-site support through trained and qualified engineers;
(iii) periodic (quarterly) systems health checks;
(iv) logistics for any necessary spare parts and media required.

**Note:* *Incident or Support Case is a technical problem affecting normal operation of equipment.*

In more detail, the Awarded Bidder should implement the following tasks:

4.2.1 Preliminary evaluation.

Within one week of contract signing, service provider should make a preliminary evaluation of the status for all the equipment, that will include (i) health check of all equipment part of central IT infrastructure; (ii) collect logs of all equipment; (iii) check status of applied patches and fixes recommended by the vendors. Based on this evaluation, service provider will prepare a report with the findings and the actions to be taken for the proper operation of all equipment. Part of the proposal should be included the methodology and a check list with approximate scheduling.

4.2.2 Periodic checks.

Service provider apart of almost real time monitoring should perform periodically health checks during which will complete the following activities: (i) physical check of equipment; (ii) collection of logs from equipment; (iii) application of any patch, fix recommended by vendors; (iv) install critical firmware updates recommended by vendors for immediate installation.

Periodic checks will be done within the last week of each quarter and service provider will provide the End-User with a document with findings, logs and all activities performed. The quarterly document will also include the ticket records of all support cases opened during the quarter and their statuses.

4.2.3 Case logging and incident resolution.

Service provider and vendors acknowledge a support incident by logging a support case, communicating the case ID to the End-User, and confirming the incident severity and time requirements for commencement of remedial action. Each case will be recorded and each step till the resolution of the incident will be documented.

4.2.4 Remote problem diagnosis and support.

Once the end-user has placed a call and it has been acknowledged, service provider and vendors should work to isolate the incident and to remotely troubleshoot, remedy, and resolve the incident with the End-User. Prior to any on-site assistance, service provider may initiate and perform remote diagnostics using electronic remote support solution to access covered products or may use other means available to facilitate remote incident resolution. Based on the problem diagnoses and remote assistance the incident may be resolved or may require further actions.

4.2.5 On-site hardware support.

For hardware incidents that cannot be resolved remotely, service provider assigns an authorized representative to provide on-site technical support on covered hardware products to return them to operating condition. Once the technical personnel arrive at the NAIS site, it may continue troubleshooting until the problem related to the central IT infrastructure is resolved or successfully diagnosed and the necessary steps to its resolutions are priory agreed with the end-user.

In addition, at the time of on-site technical support delivery, service provider may: (i) install available engineering improvements for covered hardware products to help ensure proper operation of the hardware products and maintain compatibility with supplied hardware replacement parts; (ii) install available firmware updates defined by vendor that are required to return the covered product to operating condition or to maintain supportability.

End-User and service provider should strictly follow all measures in place by the Government of Albania against spread of Covid-19 virus. It is under the service provider's responsibility to ensure that the authorized representative is fully instructed and follows the measures during any interventions in performing on-site support activities based on NAIS regulations.

4.2.6 Replacement parts and materials.

Contractor and vendors provide free of charge genuine replacement parts and materials necessary to maintain the covered hardware product in operating condition, including parts and materials for available engineering improvements required by vendors to assure supportability of the product.

Replacement parts provided under hardware support will be unit replacements or new or functionally equivalent to new in performance and reliability and warranted as new. Replaced (defective) parts will be returned to their corresponding vendor.

All equipment installed have been configured with redundant hardware options on all critical components such as power supplies, controllers, hard disc drives, memories, etc. as well as on logical configuration such as redundant roles RAID protection and continuous backup and restore. However, ensuring fast defective part replacement is crucial in maintaining the central site in normal operation.

4.2.7 Software Support.

The equipment listed in Section 3 does have software installed. For software products covered by the required support service, service provider and vendors have to provide corrective support to resolve identifiable software product problems, support to help identify problems and provide assistance in troubleshooting problems and determining configuration parameters for supported configurations.

Software support will include the license-to-use software updates from their manufactures. Part of the support delivery should be recommended software update method and recommended documentation on upgrade method.

For networking and security products, service provider and vendor have to provide real-time threat intelligence updates to block and prevent advanced cyber threats.

Service provider has to provide information, as commercially available by vendors, on current product features, known problems and available solutions, and operational advice and assistance.

4.2.8 Incident severity levels.

- ✓ Severity 1 -critical business impact: For example, production environment down: production system or production application down/critically impacted; data corruption/loss or risk; business continuity severely affected; safety and security issues.
- ✓ Severity 2 -limited business impact or business risk: For example, production environment available but some functions limited or degraded; severely restricted use; critical nonproduction environment or system issue.
- ✓ Severity 3 -no business impact: For example, nonproduction system (such as test system) or noncritical issue; work around in place, installations, questions, or requests for information or guidance.

SLAs for incident's resolution as per severity levels are defined as follows:

Feature Required	Severity 1	Severity 2	Severity 3
Access for case logging	24 x 7, Every day, holidays included		
Case logging Window	24 x 7, Every day, holidays included	24 x 7, Every day, holidays included	8:00 a.m. and 5:00 p.m., business days
Case logging requirements	Detailed Incident Description on the affected equipment		
Phone Response (remote)	Remote response 24x7 15m call back	Remote response 24x7 2-hour call back call back	Remote response, Next-Business-Day call back
E-mail Response (remote)	24 x 7, Every day, holidays included	24 x 7, Every day, holidays included	8:00 a.m. and 5:00 p.m., business days
On-site response (Hardware)	within 4-hour on-site	4-hour on-site	Next-Business-Day on-site
Parts replacement	Best effort by service provider and vendor. Should not compromise operation		
Parts replacement window	24 x 7, Every day, holidays included		Next-Business-Day
Software support	24 x 7, Every day, holidays included		Next-Business-Day
Automated incident logging	Should be available through installation of vendor's proprietary service tools		

Repair is considered complete upon the verification that the hardware malfunction has been corrected or that the hardware has been replaced.

4.2.9 Accepted Support Service limitations.

Activities such as, but not limited to, the following are excluded from the support:

- Unauthorized attempts by third-party personnel to install, repair, maintain, or modify hardware, firmware, or software;
- Services required due to improper treatment or use of the products or equipment;
- Non-designated usage of hardware or software, or usage thereof in contradiction with the recommendations from the vendors;
- Troubleshooting for interconnectivity or compatibility problems;

4.2.10 Communication between parties.

All communication by the parties should be recorded and documented accordingly. Only authorized representatives should have access on the communications.

For this purpose, End-User and service provider assign authorized representatives identified with name, surname, position within organization, telephone number, e-mail address and office address.

E-mail address and Call Center telephone numbers of the vendors for the support purposes should be available for both parties.

4.2.11 Real time monitoring

All equipment's should be monitoring in real time events and categorized based on its severity. Automatic rules should be defined to send alerts accordingly. The service provide should propose accordingly how exactly will be performed such activity, tools to be used, what will be monitored, personnel that will be in charge of configuration/ monitoring and important rules to be described how they will be configured.

5. Required Technical personnel

For the above activities the service provider should include at least 5 personnel with adequate experience and technical competence. The personnel should be aware of the business continuity procedures and participate in quarterly drills to provide prompt response in case of incidents. A documented report should be provided to the end-user after the drill procedure.

Position	Key qualification
Project Technical Manager (1)	Graduate Degree in IT/Computer Science, Engineering or Management.
	PMP, IPMA, Prince 2 Practitioner or alternative internationally recognized certificate with validity and certification process through testing centers.
	Internal staff of Proposer Bidder for at least one year.
	Experience: Minimum of 6 years of experience in managing IT projects up to successful completion, including maintenance and support services.
	Excellent written and spoken Albanian and English skills.
Server Technical Specialist (4)	Graduate Degree in in IT/Computer Science, Engineering.
	Extended proven experience with technologies such as HPE, Microsoft, KEMP and Fortinet (certification for each of the technologies will considered during the technical evaluation)
	Internal staff of Proposer Bidder for at least one year.
	Experience: Minimum of 4 years of experience in managing data center projects up to successful completion and extended experience with troubleshooting and proper maintance. ISO27001 or ITIL standards experience are considered during the technical evaluation.
	Excellent written and spoken Albanian and English skills.

6. Reporting and Expected Deliverables:

Instalments	Quantity	Conditions
1st installment	20%	▪ After submission of 1st and 2nd Quarterly Reports (2022) as per the Maintenance and Support requirements 05 Jul 2022
2nd installment	30%	▪ After submission of 3rd and 4th Quarterly Reports (2022) as per the Maintenance and Support requirements 20 Dec 2022
3rd installment	50%	▪ After submission of 1st, 2nd, 3rd, and 4th Quarterly Reports (2023) as per the Maintenance and Support requirements, and ▪ Handover document to government counterparts 20 Dec 2023

7. Special Conditions:

Considering the maintenance and support service continues for one additional year beyond the STAR3 project lifespan prepayment of the service will be applied under the condition of quarterly report presentation from the service provider to UNDP.

A MoU on OSSIS sustainability and Exit Strategy will be signed with the key counterpart institutions at central level will stipulating roles and responsibilities of MOI and NAIS related to OSSIS.