



Government
eProcurement
System

eProcurement System Government of India

Tender Details

Date : 06-Nov-2025 05:30 PM

Print

Basic Details

Organisation Chain	Office of the CAG of India AE-Punjab-Chandigarh - CAG		
Tender Reference Number	ITGD/2025/02		
Tender ID	2025_CAG_884164_1	Withdrawal Allowed	Yes
Tender Type	Open Tender	Form of contract	Lump-sum
Tender Category	Services	No. of Covers	2
General Technical Evaluation Allowed	No	ItemWise Technical Evaluation Allowed	No
Payment Mode	Offline	Is Multi Currency Allowed For BOQ	No
Is Multi Currency Allowed For Fee	No	Allow Two Stage Bidding	No

Payment Instruments

Offline	S.No	Instrument Type
	1	Demand Draft
	2	Bankers Cheque

Cover Details, No. Of Covers - 2

Cover No	Cover	Document Type	Description
1	Fee/PreQual/Technical	.pdf	Technical bid
2	Finance	.xls	Financial Bid

Tender Fee Details, [Total Fee in ₹ * - 0.00]

Tender Fee in ₹	0.00		
Fee Payable To	Nil	Fee Payable At	Nil
Tender Fee Exemption Allowed	No		

EMD Fee Details

EMD Amount in ₹	15,000	EMD Exemption Allowed	Yes
EMD Fee Type	fixed	EMD Percentage	NA
EMD Payable To	PAO AG AE PUNJAB	EMD Payable At	CHANDIGARH

[Click to view modification history](#)

Work /Item(s)

Title	Resolutions of vulnerabilities/bug fixation and data migration of websites to NGC Meghraj 2.0				
Work Description	Resolutions of vulnerabilities/bug fixation and data migration of websites to NGC Meghraj 2.0				
Pre Qualification Details	Please refer Tender documents.				
Independent External Monitor/Remarks	NA				
Show Tender Value in Public Domain	No				
Tender Value in ₹	0.00	Product Category	Miscellaneous Services	Sub category	NA
Contract Type	Tender	Bid Validity(Days)	120	Period Of Work(Days)	NA
Location	plot number 20 Sector 17 E chandigarh	Pincode	160017	Pre Bid Meeting Place	NA
Pre Bid Meeting Address	NA	Pre Bid Meeting Date	NA	Bid Opening Place	plot number 20 Sector 17 E chandigarh

Should Allow NDA Tender	No	Allow Preferential Bidder	No	
--------------------------------	----	----------------------------------	----	--

Critical Dates

Publish Date	06-Nov-2025 06:30 PM	Bid Opening Date	02-Dec-2025 11:00 AM
Document Download / Sale Start Date	06-Nov-2025 06:30 PM	Document Download / Sale End Date	01-Dec-2025 11:00 AM
Clarification Start Date	06-Nov-2025 06:30 PM	Clarification End Date	14-Nov-2025 05:30 PM
Bid Submission Start Date	06-Nov-2025 06:30 PM	Bid Submission End Date	01-Dec-2025 11:00 AM

Tender Documents

NIT Document	S.No	Document Name	Description	Document Size (in KB)	
	1	Tendernotice_1.pdf	NIT	1390.64	
Work Item Documents	S.No	Document Type	Document Name	Description	Document Size (in KB)
	1	Additional Documents	BOQ.xls	Financial bid	241.50

Bid Openers List

S.No	Bid Opener Login Id	Bid Opener Name	Certificate Name
1.	sumitk.pjb.ae@cag.gov.in	Sumit Kumar	Sumit Kumar
2.	karans.pjb.ae@cag.gov.in	Karan Singh	KARAN SINGH
3.	devendras.pjb.ae@cag.gov.in	Devendra Singh	DEVENDRA SINGH

GeMARPTS Details

Reason for non availability of GeMARPTS ID	Urgent nature of Procurement
Remarks	No drop down
Document Name	report_GEM_GARPTS_03112025_B2Z361OHGP2C.pdf
Document Size (in KB)	49.65

Tender Properties

Auto Tendering Process allowed	No	Show Technical bid status	Yes
Show Finance bid status	Yes	Stage to disclose Bid Details in Public Domain	Technical Bid Opening
BoQ Comparative Chart model	NIL	BoQ Compartive chart decimal places	2
BoQ Comparative Chart Rank Type	NIL	Form Based BoQ	No

TIA Undertaking

S.No	Undertaking to Order	Tender complying with Order	Reason for non compliance of Order
1	PPP-MII Order 2017	Agree	
2	MSEs Order 2012	Agree	

Tender Inviting Authority

Name	DAG (Admn)
Address	plot number 20 Sector 17 E chandigarh

Tender Creator Details

Created By	Karan Singh
Designation	SAO
Created Date	04-Nov-2025 04:25 PM



कार्यालय महालेखाकार (लेखा एवं हक़) पंजाब एवं यू टी , चंडीगढ़

प्लॉट संख्या 20, सेक्टर 17-ई , चंडीगढ़

टेंडर संख्या : ITGD/2025/02

वेबसाइट :- <https://cag.gov.in/ae/punjab/en>

ईमेल :- agaepunjab@cag.gov.in

क्र.- ITGD/Tender/2025/02/26

दिनांक : 04-11-2025

निविदा आमंत्रण सूचना

कार्यालय महालेखाकार (लेखा एवं हक़) पंजाब एवं यू टी , चंडीगढ़ में वेबसाइट **agpunjabpension.cag.gov.in** और **agpunjabgpf.cag.gov.in** में **Resolution of Vulnerabilities/ bug fixation and data migration of websites to NGC Megraj 2.0** हेतु बोलियां आमंत्रित करता है। निविदा जिसमें पूर्व योग्यता शर्तें एवं कार्यों का विवरण आदि सम्मिलित हैं <https://cag.gov.in/ae/punjab/en/tenders> and www.eprocure.gov.in and www.gem.gov.in से डाउनलोड किये जा सकते हैं तथा पोस्ट/कॉरियर या व्यक्तिगत रूप से प्रवर उप महालेखाकार (प्रशा.), कार्यालय महालेखाकार (लेखा एवं हक़) पंजाब एवं यू टी , चंडीगढ़ को आवश्यक दस्तावेज सहित निर्धारित तिथि तक जमा किये जा सकते हैं। बोली दस्तावेजों का कोई मूल्य नहीं है तथा अग्रिम की राशि **Rs.15,000/- (रूपये पंद्रह हजार) है।**

महत्वपूर्ण तिथियां:-

वृत्तांत	तिथि
निविदा के प्रकाशन की तिथि	06/11/2025
निविदा से सम्बंधित प्रश्न / सवाल की अंतिम तिथि	14/11/2025
बोली जमा करने की अंतिम तिथि	01/12/2025- 11:00 बजे तक
तकनीकी बोली खुलने की तिथि	02/12/2025- 11:00 बजे
वित्तीय बोली खुलने की तिथि	03/12/2025- 11:00 बजे

Sd/-

उपमहालेखाकार(प्रशा.)

**कार्यालय महालेखाकार(ले व हक़)
पंजाब एवं यू.चण्डीगढ़।.टी**



OFFICE OF THE ACCOUNTANT GENERAL (A&E), PUNJAB & UT., CHANDIGARH

Plot no. 20, Sector 17-E, Chandigarh

Tender No: ITGD/2025/02

Website :- <https://cag.gov.in/ae/punjab/en>

Email :- agaepunjab@cag.gov.in

No- ITGD/ Tender/2025/02/26

Date : 04-11-2025

NOTICE INVITING TENDER

The office of the Accountant General (A&E), Punjab & UT. Chandigarh invites bids for **Resolution of Vulnerabilities/ bug fixation and data migration of websites to NGC Megraj 2.0** of agpunjabpension.cag.gov.in & agpunjabgpf.cag.gov.in. Tender/bid document containing conditions of prequalification, detailed scope of work, etc., can be downloaded from <https://cag.gov.in/ae/punjab/en/tenders> and www.eprocure.gov.in and www.gem.gov.in and submitted the same personally or through post/courier along with required documents to the DAG (Admn) O/o the A.G.(A&E), Punjab & UT, Chandigarh, Pin-160017.

The cost of bid document is Nil and EMD is **Rs15,000/- (Rupees Fifteen Thousand only)**.

Key Events & Dates

Events	Dates
<i>Date for publication of NIT</i>	06/11/2025
<i>Last date for receipt of Queries from bidders</i>	14/11/2025
<i>Last date for submission of bids</i>	01/12/2025 up to 11:00 hrs
<i>Opening of technical bids</i>	02/12/2025 at 11:00 hrs
<i>Opening of financial bids</i>	03/12/2025 at 11:00 hrs

Sd/-

Deputy Accountant General (Admn),

Office of AG (A&E), Punjab & UT, Chandigarh

**OFFICE OF THE ACCOUNTANT GENERAL (A&E), PUNJAB AND U.T., CHANDIGARH -
160017.**

1. The office of the Accountant General (A&E) Punjab & UT, Chandigarh invites bids for **Resolution of Vulnerabilities/ bug fixation and data migration of agpunjabpension.cag.gov.in (As Per Annexure A)& agpunjabgpf.cag.gov.in (As Per Annexure B)**

2. Bid document containing conditions of eligibility of prequalification, detailed scope of work etc. can be downloaded from from <https://cag.gov.in/ac/punjab/en/tenders> and www.eprocure.gov.in and www.gem.gov.in.

3. Cost of Tender/bid document

Cost of the Bid document is Nil.

For details the bidders may go through the Bid Documents.

BID DOCUMENT

1. BACKGROUND, SCOPE OF WORK AND INSTRUCTIONS TO VENDORS

1.1. Introduction

The website **agpunjabgpf.cag.gov.in & agpunjabpension.cag.gov.in** has been hosted on NIC server, the security audit of both the websites were conducted and several bugs has been identified, the same needs to be resolved and thereafter the website data needs to be migrated from old NIC server to latest NGC meghraj 2.0

2. SCOPE OF WORK

Scope of Work:

The scope of work will include the following :-

1. The security audit of the websites has been conducted by a already hired CERT empanelled vendor and several bugs has been identified listed as Annexure 1 & 2, your firm will be responsible for Resolution of Vulnerabilities/ bug fixation of agpunjabpension.cag.gov.in **(As Per Annexure 1)** & agpunjabgpf.cag.gov.in **(As Per Annexure 2)**.
2. After the above bugs are fixed, then the second round of security audit will be conducted by the already hired CERT empanelled vendor and the bugs/errors/issues (if any) identified in the second round, the same needs to be resolved by your firm and the process will be repeated till the security audit is successfully completed and security audit certificate is issued by the vendor
3. After obtaining the security audit Certificate, the website data of (agpunjabgpf.cag.gov.in and agpunjabpension.cag.gov.in) which presently being hosted by NIC on their old servers, and now as the older servers has become obsolete therefore, the website data is to be migrated on the new servers of NIC cloud divisin i.e. NGC Megraj 2.0. The specifications/details of the new infrastructure is mentioned in Annexure 3. The database (MariaDB) needs to be configured on the new servers and the website to be made operational with all the functionalities of existing username/passwords logins etc.

“Annexure 1”

S.no.	Observation/Vulnerability title	CVE/CWE	Severity	Detailed observation	Recommendation
1	HTML Injection	CWE-79	Critical	This vulnerability occurs when the user input is not correctly sanitized, and the output is not encoded. An injection allows the attacker to send a malicious HTML page to a victim. The	--All input fields must sanitise the input given to them before sending it to the server.

				targeted browser will not be able to distinguish (trust) the legit from the malicious part and consequently will parse and execute all as legit in the victim context.	
2	Reflected Cross-site scripting (XSS)	CWE-79	High	Reflected XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.	--All input fields must sanitise the input given to them before sending it to the server. Note: Fix this issue throughout the application.
3	CSS Injection	CWE-79	High	Observed that application allows user-supplied CSS to interfere with the application's legitimate stylesheets. Injecting code in the CSS context may provide an attacker with the ability to execute JavaScript in certain conditions, or to extract sensitive values using CSS select or and functions able to generate HTTP requests.	All input fields must sanitise the input given to them before sending it to the server. Note: Fix this issue throughout the application.
4	Session Hijacking	CWE-384	High	The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server. Once the user's session ID has been accessed, the attacker can masquerade as that user and do anything the user is authorized to do on the network.	--Make sure that all session identifiers are transmitted over an encrypted protocol. --Terminate/regenerate the session if the session token is transmitted insecurely (either in clear text or as part of the URL). --Enforce the Secure and Http Only flags on sensitive cookies using a Web Application Firewall. --Ensure that session identifiers are transmitted only using the SSL session where they originated. Track

				sessions across SSL renegotiations and integrate with framework solutions to support common SSL termination/re-encryption architectures. Note: Fix this issue throughout the application.
5	No Session Timeout	CWE-613	Medium	Session time out represents the event occurring when a user does not perform any action on a website during a interval (defined by web server). This timeout defines the amount of time a session will remain active in case there is no activity by the user, closing and invalidating the session upon the defined idle period since the last HTTP request received by the web application for a given session ID. Set session timeout to the minimal value possible depending on the context of the application. Avoid "infinite" session timeout. Prefer declarative definition of the session timeout in order to apply global time out for all application sessions. Trace session creation/destroy in order to analyse creation trend and try to detect abnormal session number creation.
6	Browser Cache Weakness	CWE-525	Medium	If sensitive information is displayed to the user (such as their address, credit card details, Social Security Number, or username), then this information could be stored for purposes of caching or history, and therefore retrievable through examining the browser's cache or by simply pressing the browser's "Back" button. The "Back" button can be stopped from showing sensitive data. This can be done by: Delivering the page over HTTPS & Setting Cache Control: must-cache or by simply pressing the revalidate.
7	Sensitive Information exposure through URL	CWE-200	Medium	Information exposure through query strings in URL is when sensitive data is passed to any parameters in the URL. This allows attackers to obtain sensitive data such as usernames, passwords, tokens (auth X), data to base details, and any other potentially sensitive data. Simply The application should never transmit any sensitive information within the URL query string. It may also be necessary to modify the corresponding server-side form handler to ensure that submitted

				using HTTPS does not resolve this vulnerability.	information are properly retrieved from the message body, rather than the URL.
8	Frame Injection	CWE-601	Medium	Frame injection, which occurs when a frame on a vulnerable web page displays another web page via a user-controllable input.	--Where possible do not use users' input for URLs. --If you definitely need dynamic URLs, make a list of valid accepted URLs and do not accept other URLs. Ensure that you only accept URLs which are located on accepted domains.

Annexure-2

S.no.	Observation/Vulnerability title	CVE/CWE	Severity	Detailed observation	Recommendation
1	HTML Injection	CWE-79	Critical	This vulnerability occurs when the user input is not correctly sanitized, and the output is not encoded. An injection allows the attacker to send a malicious HTML page to a server. The targeted browser will not be able to distinguish (trust) the legit from the malicious part and consequently will parse and execute all as legit in the victim context.	--All input fields must sanitise the input given to them before sending it to the server.
2	Frame Injection	CWE-601	Medium	Frame injection, which occurs when a frame on a vulnerable web page displays another webpage via a user-controllable input.	--Where possible do not use users' input for URLs. --If you definitely need dynamic URLs, make a list of valid accepted URLs and do not accept other URLs. Ensure that you only accept URLs

					which are located on accepted domains.
3	No Session Timeout	CWE-613	Medium	Session time out represents the event occurring when a user do not perform any action on a website during a interval (defined by web server). This timeout defines the amount of time a session will remain active in case there is no activity by the user, closing and invalidating the session upon the defined idle periods in the last HTTP request received by the web application forgiven session ID.	Set session time out to the minimal value possible depending on the context of the application. Avoid "infinite" session time out. Prefer declarative definition of the session time out in order to apply global time out for all application sessions. Trace session creation/destroy in order to analyse creation trend and try to detect abnormal session number creation.
4	Misconfigured 'Strict-Transport-Security' Header	CWE-693	Low	HTTP Strict Transport Security (HSTS) is a response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.	--Depending on the framework being used the implementation methods will vary, however it is advised that the 'Strict-Transport Security' header be configured properly on the server. --Strict-Transport-Security: max-age should be >= 31536000; Include Sub Domains

“Annexure 3”

#	Type	Remarks	Cloud	Configuration	Total Qty	NGC SKU (For Commercial Use)
1	Virtual Machine (Ubuntu - Bastion Host)	Bastion Host	Private Cloud	2 vCPU, 8 GB Memory	1	VM of 2 vCPU, 8 GB RAM
2	Virtual Machine- (RHEL) - Web	AG Punjab Pension	Private Cloud	2 vCPU, 4 GB Memory	1	2vcpu, 4 GB Memory
4	Virtual Machine- (RHEL) -DB	AG Punjab Pension	Private Cloud	2 vCPU, 4 GB Memory	1	2vcpu, 4 GB Memory
6	RHEL Licenses	RHEL Licenses	Private Cloud	2 vCPU RHEL	2	RHEL 2 Core License
7	Storage - Boot Volume	Boot Volume	Private Cloud	300 GB	300	Block Storage - SSD - 100GB minimum 150 IOPS
8	Storage - Block (Additional Storage)	Sum of VM Additional Disk and DB storage size	Private Cloud	200 GB	200	Block Storage - SSD - 100GB minimum 250 IOPS
9	Backup as a service	Sum of Boot Volume and Additional Disk	Private Cloud	500 GB	500	Per GB /month
10	Public IP	Public IP	Private Cloud	Public IP	1	Public IP
11	Application load Balancer		Private Cloud	ALB - 50 Mbps	1	Throughput in mbps
12	WAF		Private Cloud	ALB - 50 Mbps	1	Throughput in Mbps
13	Next Gen Firewall		Private Cloud	ALB - 50 Mbps	1	Throughput in Mbps
14	Anti Malware		Private Cloud	All VMs	3	Anti Malware per VM
15	Vulnerability Scanning		Private Cloud	All VMs	3	Vulnerability scanning - per VM

3. TIME SCHEDULE OF THE PROJECT

The work should be completed within a time frame of **30 days** from the date of commencement. Extension of time frame shall be considered on genuine grounds and decision of the Accountant General. However, no extra cost shall be payable for the extended period.

4. PROCEDURE FOR SUBMISSION OF BIDS

In order to participate in the bidding process, bidders should follow the procedure described below for submitting their bids. Failure to do so may result in the bid being eliminated at the examination stage as non-responsive.

4.1. Submit sealed envelopes containing Technical bid and Financial bid *separately* in the following manner:

4.1.1. Envelope I – Technical Bid —

Each of Technical Bid (Eligibility Criteria) comprising all mentioned necessary documents in Annexure- along with all information requested by Purchaser in para 4.2 of this bid.

a) Technical Bid should be a complete document, bound as a volume and placed in separate sealed envelope. Every page of the bid shall be numbered.

b) The envelope containing the Technical Bid should be superscribed as below:

“TECHNICAL BID FOR TENDER NO. _____”.

4.1.2. Envelope II---Financial Bid.

a) Financial Bid should be a complete document, bound as a volume and placed in separate sealed envelope. It shall be certified that the rates quoted in the financial bid shall remain valid for a period of **120 (one hundred twenty) days**.

b) The envelope containing the Financial Bid should be superscribed as below:

“FINANCIAL BID FOR TENDER NO. _____

4.1.3. Amendment of Tender/bid document

At any time prior to the last date for receipt of bids, Purchaser may, for any reason, whether at its own initiative or in response to a clarification requested by prospective bidder(s), modify the tender document by an amendment.

4.1.4. Financial bid of only those Agencies/firms who fulfill the terms & Conditions as specified in section 4.2 and essential parameter of tender document will be opened separately which is as per dates specified in tender. However, if any change in schedule of opening of financial Bid, it will be informed to qualifying firms through E-Mail only.

Therefore, the e-mail id of authorized signatory must be mentioned in Performa provided in para 5.3

4.2. Documents comprising the bid-

The bids prepared by the Bidder(s) shall comprise of the following components:

A. Technical bid as per criteria specified below to be submitted before last date of submission of bid along with the following:

1. The bidder must be a company registered under the Companies Act, 1956/2013.
2. Copy of GST certificate
3. Copy of PAN
4. EMD in the form of account payee DD/Banker's Cheque in favour of Pay and Accounts Officer O/o PAG (A&E) Punjab, Chandigarh has to be submitted along with bid documents. *(Bid validity should be 120 days after last date of opening of financial bid.)*
5. EMD should be placed in the Technical bid 'Original'.
6. Person signing the bid shall bind the bidder as the 'Constituted Authority of the company'.
7. At least 3 satisfactory performance certificate for websites related work at any Govt./PSU/semi govt. in the last 3 years.
8. CA verified Turnover certificate of the firm of last 3 years.
9. Letter of undertaking regarding acceptance of all the terms and condition of this tender document & non black listed by any Govt./semi Govt. Organization or PSU.

B. Financial Bid (Annexure-II) as per Section 4.1.2 and subsections there under to be submitted on or before last date of submission of bid

4.3. Withdrawal of Bids

The bidder may withdraw his bid after the submission of bids, provided that written notice of the withdrawal is received by Purchaser prior to the last date prescribed for receipt of bids.

4.4. Forfeiture of Bid Security

No bid may be withdrawn in the interval between the last date for receipt of bids and the expiry of the bid validity period specified by the bidder in the bid. Withdrawal of a bid during this interval shall result in forfeiture of EMD.

4.5.1. Bidder

The bidder shall designate the official mailing address, place, telephone number, fax number and email address to which all correspondence shall be sent by Purchaser.

4.5.2. Purchaser

Deputy Accountant General (Admn)

Office of the ACCOUNTANT GENERAL (A&E), PUNJAB, Lekha Bhavan,

Plot No. 20, Sector-17E,

Chandigarh – 160017.

Purchaser shall not be responsible for non receipt of any communication sent by the Bidder. All correspondence by post/email/fax should indicate the Bid Reference number and marked “**Confidential /To be opened by the Addressee only**”, as the case may be.

4.5.3. Preliminary Examination

Purchaser will examine the bids to determine whether they are complete, whether any computational errors have been made, whether required bid security has been furnished, whether the documents have been properly signed, and whether the bids are generally in order. A bid determined as not substantially responsive will be rejected by Purchaser and may not subsequently be made responsive by the bidder by correction of the nonconformity. Purchaser may waive any minor informality or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such waiver does not prejudice or affect the relative ranking of any bidder.

4.5.4. Criteria for award of Agreement

In addition to the technical competence, Purchaser will determine to their satisfaction whether the bidder(s) selected as having submitted the best evaluated responsive bid is qualified to satisfactorily perform the agreement. The decision of Purchaser shall be final in such cases. Purchaser will review the financial bids of only those bids found technically suitable. Bids that are not substantially responsive are liable to be disqualified at Purchaser's discretion. Purchaser reserves the right to reject any bid without assigning any reason.

5. GENERAL CONDITIONS OF AGREEMENT

5.1. Performance bank guarantee

Within Seven (7) days after the receipt of notification of award of the agreement from Purchaser, the successful bidder shall furnish performance guarantee at 10% of bid value to the Purchaser in the form of Account Payee Demand Draft, Fixed Deposit Receipt from a Commercial bank, Bank Guarantee [including e-Bank Guarantee] from a Commercial bank or online payment in an acceptable form safeguarding the purchaser's interest in all respects.. The performance guarantee shall be valid for a period of 2 months from the last date of expiry of the warranty period of the project. The successful bidder shall renew the bank guarantee to ensure its validity up to the end of this period.

5.2 Warranty

The Service Provider shall submit a warranty for successful operation of the both the websites work after completion of the project. The warranty **MUST** be for **12 months** from the date of completion of the work.

5.3 Payment Terms

No payment towards the agreement shall accrue until after the performance bank guarantee bond envisaged in section 5.1 has been furnished. Payment under the agreement shall be made only for the work completed with reference to the at 5.4 below.

5.4 Payment

Payment will be made after completion of work i.e. successful migration of both the websites on the new servers, and successful testing of this office. All bugs of security audit must be resolved in all rounds of security audit and the security audit certificate is obtained, further the migration work must also be completed. The payment will be made by this office, only after all the works mentioned in "Scope of work" are successfully completed, and tested by this office.

5.5 Prices

The prices quoted for the components of services and optional services shall be firm throughout the period of agreement and shall not be subject to any escalation.

5.6 Taxes and Duties

The quoted Rate/Cost should be inclusive of all levies/taxes like Service tax, Educational cess, Sales Tax, Transportation customs, Excise, travelling charges etc, if any.

5.7 Legal Jurisdiction

For any dispute or legal matters arising out of or in relation to this agreement, the jurisdiction shall be Chandigarh only.

Annexure I

Technical Bid

Development of Web based Cloud utility for Pension revision cases AT THE OFFICE OF ACCOUNTANT GENERAL (A&E) PUNJAB & UT, CHANDIGARH (supporting documents for Sr. No. 1-13 must be enclosed)

1	Name of the Company	
2	Address (with Tel. No., Fax no. & e-mail address)	
3	Contact Number	
4	(a) Registration Number	
	(b) PAN Number	
	(c) GSTN no.	
5	:- Details of EMD Deposited and cost of Tender	

Sr. no.	Particular (copy of supporting documents duly self attested)	Enclosed (Yes or no)	Attached at page no. (Page numbering Cumpolsory)
6	Registration certificate of company registered under the Companies Act, 1956/2013		
7	CA verified Turnover certificate of the firm of last 3 years.		
8	Person signing the bid shall bind the bidder as the 'Constituted Authority of the company/firm.		
9	Letter of undertaking regarding the company is not black listed by any Govt./semi Govt.		

	Organization or PSU. (Annexure III)		
10	Letter of undertaking regarding acceptance of all the terms and condition of this tender document.		
11	At least three Satisfactory performance certificate regarding development / modification / maintenance php/oracle based system at any Govt./semi Govt. organization or PSU in last 3 years.		

Declaration

I hereby certify that the information furnished above is full and correct to the best of our knowledge. We understand that in case found any deviation in the above statement at any stage, the company will be black-listed and will not have any deal with the Govt. offices in future. I also certify that the period of validity of this Bid is 120 days from the date of opening of the Financial Bid.

(Signature of authorized signatory)

Annexure II

Financial Bid

Development of Web based Cloud utility for Pension revision cases AT THE OFFICE OF ACCOUNTANT GENERAL (A&E) PUNJAB & UT, CHANDIGARH

Format for the submission of bid:-

Sr.No	Item	Cost combined rate of both the works. (In INR)
1	Resolution of Vulnerabilities/ bug fixation and data migration of agpunjabpension.cag.gov.in & agpunjabgpf.cag.gov.in (As Per Annexure A & B) And data migration of the websites to the new NGC Megraj 2.0 including 12 months onsite maintenance warranty from final signoff. Applicable Taxes	
	Grand Total	

Grand Total (in words) :-

.....

Signature and Seal of authorized signatory

**FORMAT OF UNDERTAKING, TO BE FURNISHED ON COMPANY
LETTER HEAD WITH REGARD TO BLACKLISTING/ NON-
DEBARMENT, BY ORGANISATION**

**UNDERTAKING REGARDING BLACKLISTING / NON –
DEBARMENT**

To,

Deputy Accountant General (Admn),
Office of the Accountant General (A&E), Punjab & UT.
Chandigarh-160017

Sir,

We hereby confirm and declare that we, M/s_____, is not blacklisted/ De-registered/ debarred by any Government department/ Public Sector Undertaking/ Private Sector/ or any other agency for which we have Executed/ Undertaken the works/ Services in past.

There are no complaints against us regarding delayed supply and refusal of supply for which supply order granted by the client or Govt. department.

I hereby accept all the terms and conditions of this tender.

For_____

Authorised Signatory

Date:

LETTER OF AUTHORISATION FOR ATTENDING BID OPENING

Subject: - Authorization for attending bid opening on (Date) in the Tender for purchase of servers in the office of the Accountant General (A&E) Punjab & UT, Chandigarh

Following persons are hereby authorized to attend the bid opening for the tender Mentioned above on behalf of (Bidder) in order of preference given below.

Order Preference	of	Name	Specimen Signature
1			
2			

Signature of the Tenderer
Or Officer authorized to sign
the bid Documents on behalf
of the Tenderer

Note:-

1. Maximum of two representatives will be permitted to attend bid opening in cases where it is restricted to one first preference will be allowed.
2. Permission for entry to the hall where bids are opened may be refused in case authorization as prescribed above is not received.

Signature of the Tenderer & Seal

Check List

1. The **Technical Bid** (Eligibility Criteria) 'original' and 'copies' should be placed in one sealed **Envelope I** super scribing '**Technical Bid for _____ Dated _____**' as per requirements mentioned at **4.1.1 and 4.2 and Annexure I**. Please ensure that all the documents as prescribed in this Bid Document
2. The cost of the Bid Document is **Nil**.
3. All bids must be accompanied by EMD in the form of Cheque/Demand draft of **Rs 15,000/- (Rupees Fifteen Thousand only)**. The EMD should be submitted in the Sealed Envelope of Technical Bid "Original"
4. The '**Financial Bid**' should be as per the requirements mentioned at **Annexure II** and other relevant instructions and placed separately in the sealed Envelope II duly superscribed as Financial bid for Tender no. _____
5. It should be ensured that requirement(s) of all relevant sections and sub-sections of the tender document have been complied with and all the pages of bid has been numbered.

Key Events & Dates

Events	Tentative dates
Date for publication of NIT	06/11/2025
Last date for receipt of Queries from bidders	14/11/2025
Last date for submission of bids	01/12/2025 up to 11:00 hrs
Opening of technical bids	02/12/2025 at 11:00 hrs
Opening of financial bids	03/12/2025 at 11:00 hrs

Note: The bidder shall sign all papers of the bid and also the pamphlets, drawings, client list, company profile etc before submitting his bid and all pages of tender must be page marked in numeric and total no. of page enclosed in bid should be mentioned in the covering letter.