INDIAN AVIATION ACADEMY

Information Technology Department

IAA, Vasant Kunj, New Delhi

TENDER/BID DOCUMENT

Tender/Bid ID: GEM/2024/B/4926424

For the Work of: Design, Development, Launching, Maintenance and associated services of e-Internship portal.

Estimated cost	:	**Rs. 60,60,000 /- (Rupees Sixty Lakh Sixty Thousand Only) Inclusive of GST.**
Tender Date	:	**09.05.2024**

For the Work of: Design, Development, Launching, Maintenance and associated services of e-Internship portal.

INDEX

Sl. No.	Particulars	Page No.
1	**E-NIT (Cover Page)**	1
i	Index	2
ii	e-Tender Notice	3-9
2	**General Conditions of Contract (GCC)**	10-18
3	**Special Conditions of Contract (SCC)**	19-22
4	**Scope of Work/ Qualitative Requirements/Technical Specification**	23-32
5	**Checklists and Annexures**	
i.	Checklist (Envelope I & II)- Annexure A & B	33-38
ii.	Unconditional Acceptance Letter (Annexure-I)	39
iii.	Undertaking Regarding Blacklisting (Annexure-II)	40
iv.	Proforma of E-payment (Annexure-III)	41
v.	Undertaking of Registration certificate (Annexure-IV)	42
vi.	Declaration of Net Worth Proforma (Annexure-V)	43
vii.	Affidavit of Exit Management Plan (Annexure-VI)	44
viii.	Proforma for Bank Guarantee (Annexure-VII)	45-46
ix.	Proforma for Applying Extension of Time (Annexure-VIII)	47-49
x.	Guidelines on Cyber security & audit (Annexure-IX)	50-59
xi.	Checklist for Comprehensive security audit (Annexure-X)	60-98
6	**Schedule of Quantities**	99-100

The tender documents contain **100** pages as detailed above.

Assistant manager (IT), IAA
Vasant Kunj, New Delhi

Indian Aviation Academy

Notice Inviting e-Tender/bid (2 BOT- 2 Envelope Open Tender/bid)

(Tender/Bid ID-GEM/2024/B/4926424)

NIT No: IAA/ITD/Internship/2024 **Date: 09.05.2024**

1. E-tender/bids are invited through the e-tender/biding portal by Assistant Manager (IT), IAA, Vasant Kunj, Delhi-110070, (Bid Manager) on behalf of Director, IAA, from the eligible contractors for the work of **"Design, Development, Launching, Maintenance and associated services of e-Internship portal"** for an estimated cost of **Rs. 60,60,000 /- (Rupees Sixty Lakh Sixty Thousand Only)** which is inclusive of all other charges and GST with the period of completion for Design, development & launching of Internship portal is 60 days from the date of award of work.

The tender/bidding process is online at GEM-portal URL address https://gem.gov.in or www.aai.aero. Prospective Tender/bidders may download and go through the tender/bid document.

Prospective Tender/bidders are advised to get themselves register at GEM-portal, obtain "Login ID" & "Password" and go through the instructions available in the Home page after login to the GEM-portal https://gem.gov.in or www.aai.aero.

For queries related to the tender/bid published on the portal, bidders are advised to raise query on the portal.

Tender/bid fee of **Rs. 1,770.00/- (Rupees One Thousand Seven Hundred Seventy Only) non-refundable** will be required to be paid offline in the form of Demand Draft from Nationalized or any scheduled bank (**but not from Co-operative or Gramin bank**). Tender/bid Fee in favour of **Indian Aviation Academy (NIAMAR Society)**, payable at New Delhi. The original demand draft against tender/bid fee should be posted / couriered / given in person to the concerned officials, received latest by the last date of bid submission or as specified in the tender/bid document. The details of demand draft / any other accepted instruments, physically sent, should tally with the details available in the scanned copy and the data entered during bid submission time.

CRITICAL DATA SHEET

Sl. No.	Activity	Date &Time (IST)
1	Publishing Date	09.05.2024, 2000 Hrs. IST
2	Bid Document Download / Sale Start Date	09.05.2024, 2000 Hrs. IST
3	Clarification Start Date	09.05.2024, 2000 Hrs. IST
4	Clarification End Date	16.05.2024, 1800 Hrs. IST
5	Bid Submission Start Date	09.05.2024, 1800 Hrs. IST
6	Bid Submission End Date	30.05.2024, 1800 Hrs. IST
7	Last date and time of ***physical submission*** of DD against EMD, Tender/bid Fee, Signed hard copy of IAA Unconditional Acceptance Letter to Assistant Manager (IT), IAA, Vasant Kunj, New Delhi-110070.	06.06.2024, 1800 Hrs. IST
8	Bid Opening Date: Envelope-I (PQQ & Technical)	07.06.2024, 1100 Hrs. IST
9	Bid Opening Tentative Date: Envelope-II (Financial)	14.06.2024, 1800 Hrs. IST
10	Tender/bid Fee	**Rs. 1,770** /- (**Rupees One Thousand Seven Hundred Seventy Only)(Non- Refundable)**
11	Earnest Money Deposit (EMD)	**Rs. 1,21,200/- (Rupees One Lakh Twenty One Thousand Two Hundred Only)**

2. Bid Submission:

Bids shall be submitted online at GEM portal website: https://gem.gov.in. Tender/bidder/Contractor are advised to follow the instructions available on GeM portal and apply in the bid. Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.

3. Not more than one tender/bid shall be submitted by one contactor or contractor having business relationship. Under no circumstance will father and his son(s) or other close relations who have business relationship with one another (i.e. when one or more partner(s)/director(s) are common) be allowed to tender/bid for the same contract as separate competitors. A breach of this condition will render the tender/bids of both parties liable to rejection.

4. Tender/bidder who has downloaded the tender/bid from GEM Portal website **https://gem.gov.in**, shall not temper/modify the tender/bid form including downloaded price bid template in any manner. In case if the same is found to be tempered/modified in any manner, tender/bid will be completely rejected and tender/bidder is liable to be banned from doing business with Indian Aviation Academy.

5. Following 2 covers shall be submitted through online at GEM portal by the bidder as per the following schedule: -

(A) Envelope-I: **- Containing qualifying requirements of Contractor /Firm: -**

i) Agency should have Permanent Account Number (PAN) and GST Registration.

ii) Should have valid registration on the date of issue of tender/bid in appropriate class of CPWD/MES/P&T/Railways/State PWD/PSU/ Municipal Corporations & Development Authorities of Delhi, Mumbai, Chennai and Kolkata or Agency specialized in similar nature of work and Registered with Registrar of Companies / Firms / Central Govt. / State Govt. entity in India.

And

iii) Should have satisfactorily completed (Phase/Part completion of the scope of similar work in a contract shall not be considered. However, predetermined phasing of the work may be accepted) **Three works** each of **INR 24,24,000 (Rupees Twenty Four Lakh Twenty Four Thousand Only) or more**, **Two works** each of **INR 30,30,000 (Rupees Thirty Lakh Thirty Thousand Only) or more**, **One work** of **INR 48,48,000 (Rupees Forty Eight Lakh Forty Eight Thousand Only) or more,** in single contract of similar nature of works **in a single work order of amount mentioned above for each work** during last seven years ending on **31.03.2024**.

iv) **Similar nature of work** means work similar as **"Design, Development and launching of Internship and/or Online portal with online Hosting, Maintenance & associated services".**

v) Client certificate for experience should indicate the nature of work done, the value of completed work, date of start, actual date of completion and satisfactory completion of work duly supported by Award letter, Schedule of Quantities.

vi) "The value of executed works shall be brought to current costing level by enhancing the actual value of work at simple rate of 7% per annum, calculated from the date of completion to the last date of submission of bid."

vii) **Firms showing work experience certificate from non-government/non-PSU organizations should submit copy of Tax Deduction at Sources (TDS) certificate in support of their claim for having experience of stipulated value of work.**

viii) a) Should have **Annualized Average Financial Turnover** of **Rs. 9,09,000/- (Rupees Nine Lakh Nine Thousand Only) or more**, against works executed during **last three years** ending **31st March of the previous financial year**. As a proof, copy of Abridged Balance Sheet and Profit and Loss Account Statement of the firm should be submitted along with the application. Firms showing continuous losses during the last three years in the balance sheet shall be summarily rejected.

b) Also **Net worth certificate** of **Rs. 4,54,500/- (Rupees Four Lakh Fifty Four Thousand Five Hundred Only) or more**, as per Annexure-V of the Tender/bid Document should be submitted by agency.

ix) **All documents related to financial certificates i.e. turnover, copy of Abridged Balance Sheet and Profit and Loss Account Statement and net worth certificate of the firm must be submitted with a Unique Document Identification Number (UDIN). UDIN was introduced by "The Institute of Chartered Accountants of India" for the members of the institute to curb the malpractice of false certificate/attestation by the unauthorized person & to eradicate the practice of bogus certificates.**

x) **If the submitted Documents of agency are without UDIN number the bid of the agency shall be summarily rejected.**

xi) PQ Proforma as per duly filled and signed (Checklist / Annexure-A & B).

xii) Earnest Money Deposit (EMD), Tender/bid Fee, Unconditional Acceptance of IAA's Tender/bid Conditions and Digitally Signed Tender/bid Documents.

xiii) Bidders other than proprietary firm shall submit scanned copy of Authorization Letter/Power of Attorney along with copy of Certificate of Incorporation of the Company under Companies Act showing CIN/LLPIN/Name of Directors of the Company and copy of Board Resolution regarding Authority to assign Power of Attorney. Proprietary firm shall submit scanned copy of Authorization Letter/Power of Attorney only if tender is processed by a person other than proprietor.

Original/Hard copy of the same is required to be submitted to the ***Assistant Manager (IT), Indian Aviation Academy, Vasant Kunj, New Delhi-110070*** as per the timeline mentioned in **CRITICAL DATA SHEET**. ***The bidder who fails to submit the original DD towards Tender/bid fee, DD towards EMD Declaration and Unconditional Acceptance letter before the stipulated time or are not meeting IAA's tender/bid conditions then their tender/bid shall be rejected out-rightly. Any postal delay will not be entertained.***

And

(B) Envelope-II: - **The Financial e- Bid through GEM portal**

All rates shall be quoted in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender/bid document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete the **all yellow colored (unprotected) cells with their respective financial quotes and other details (such as name of the bidder etc.) as per the Schedule of Quantity/BOQ format**. No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.

Note: BOQ must be uploaded on GeM portal by bidders for bifurcation of price estimate as per Schedule of Quantities.

6. Concessions to Indian Micro & Small Enterprises (MSMEs) Units and Start Up India: -

As per the provisions given by Ministry of Micro, Small and Medium Enterprises vide F. No. 24./02/2013-Fin.1 dated 02.08.2016 for order for relaxation on prior experience and prior turnover will be given to all Startups(MSME or otherwise) companies in the similar nature of work under the service sector required document. As per the provisions (para-10) of Public Procurement Policy for MSE's Order 2012, MSEs (Micro & Small Enterprises) registered with DIC/NSIC/KVIC/KVIB/Directorate of Handicraft and Handloom etc. only following concessions shall be applicable and extended to the MSE's of same specifications under which they are register equaling tender/bid scope of work.

i) **Tender/bid Document Fee:** MSMEs Bidders seeking exemption and benefits should upload digitally signed self-attested scanned copy of valid Registration Certificate, giving details of such

validity, stores / services etc. in **Envelope-I (Fee),** failing which they run the risk of their bid being passed over as ineligible for the benefits applicable to MSME's. The benefits to MSMEs shall be available only for the Goods/Services produced and provided by MSEs for which they are registered.

ii) **(a) Exemption of Earnest Money Deposit (EMD)**: Micro and Small Enterprises (MSEs) as defined in MSE Procurement Policy issued by Department of Micro, Small and Medium Enterprises (MSME)" are exempt from submission of EMD (Bid security). Bidders claiming exemption of EMD are however required to submit a signed Bid securing declaration accepting that if they withdraw or modify their Bids during the period of validity, or if they are awarded the contract and they fail to sign the contract, or to submit a performance security before the deadline defined in the request for bids document, they will be suspended for the period of 1 year from being eligible to submit Bids for tender/bids with Indian Aviation Academy.

(b) Implementation of micro, small and medium enterprises development (MSMED) Act, 2006.
It has been clarified that benefit to MSMEs shall not be extended to construction work as it cannot be treated as service rendered or supply of goods.
Further, it is also clarified that benefits to MSME shall be available only for the goods/ services produced and provided by MSME for which they are registered as mentioned clearly in their MSME/NSIC.

(c) Tender/bidder(s) fulfilling eligibility criteria and having valid registration with **National Small Industries Corporation (NSIC)** are exempted from tender/bid fee and earnest money deposit (EMD). Bidder(s) having valid NSIC registration certificate for relevant scope of work are required to upload NSIC certificate in **Envelope-I (Fee folder)** to qualify for exemption of tender/bid fee and EMD, while submitting the online tender/bid.

Note - During bid evaluation, EMD exemption shall be granted to NSIC registered bidder firm. In case NSIC registration certificate is found invalid during evaluation, the bid of such bidder shall be rejected.

iii) For this tender/bid MSMEs Bidders seeking exemption for tender/bid fee and EMD must submit the MSMEs certificate which that the certificate is issued for the work of **"Design, Development, Launching, Maintenance and associated services of e-Internship portal"** or of similar nature of work means work similar as **"Design, Development and launching of Internship and/or Online portal with online Hosting, Maintenance & associated services",** If it was found that the certificate is not issued for this work or similar nature of work it will presumed that the bid is submitted without tender/bid fee and the bid of the agency shall be summarily rejected.

7. Bids Opening Process is as below: -

Envelope-I:
Containing documents for PQQ & Technical bid (uploaded by the contractors/firms) shall be opened as per **CRITICAL DATA SHEET**. The intimation regarding acceptance/rejection of their bids will be intimated to the contractors/firms through GeM portal. Financial bid opening date shall be mentioned in **CRITICAL DATA SHEET** (any changes in the date shall be intimated through GEM Portal)

If any clarification needed from the bidder about the deficiency in his uploaded documents in Envelope-I, he will be asked to provide it through GEM portal. The bidder shall upload the requisite clarification/documents within time specified by IAA, failing which tender/bid will be liable for rejection.

Envelope-II:

The financial bids of the contractors / firms found to be meeting the qualifying requirements and technical criteria shall be as per **CRITICAL DATA SHEET**. (Depending on technical bid evaluation the date shall be intimated through GEM portal).

Date of opening of Envelope-II shall be intimated via GEM portal. (Depending on pre-qualification, any changes in the date shall be intimated through "GEM Portal" section). If any clarification is needed from the bidder about the deficiency in his uploaded documents in Envelope – I and he will be asked to provide it through the GEM portal. The bidder shall upload the requisite clarification /documents within time specified by IAA, failing which tender/bid will be liable for rejection.

The financial bids of the contractors/firms found to be meeting the qualifying requirements and technical criteria shall be opened and date of opening shall be communicated via GEM Portal. (Depending on Envelope-I Evaluation, any changes in the date shall be intimated through "GEM portal" section).

Any modification(s)/change(s) done by the bidder in BOQ document apart from **all yellow (unprotected cell including price and variable cost in % age) cell** quoted by him shall be summarily rejected.

Note: BOQ must be uploaded on GeM Portal by bidders for bifurcation of price estimate as per Schedule of Quantities.

8. IAA reserves the right to accept or reject any or all applications without assigning any reasons. IAA also reserves the right to call off tender/bid process at any stage without assigning any reason.

9. IAA reserve the right to disallow issue of tender/bid document to working agencies whose performance at ongoing project (s) is below par and usually poor and has been issued letter of restrain/Temporary/Permanent debar by any department of IAA. **IAA reserve the right to verify the credential submitted by the agency at any stage (before or after the award the work). If at any stage, any information / documents submitted by the applicant is found to be incorrect/false or have some discrepancy which disqualifies the firm then IAA shall take the following action:**

(a) The agency shall be liable for debarment from tender/biding in IAA for a period of 1 year, apart from any other appropriate contractual /legal action.

10. Consortium/Joint venture (JV) companies shall not be permitted. No single firm shall be permitted to submit two separate applications.

11. Purchase preference to Central Public Sector Undertaking shall be applicable as per the directive of Govt. of India prevalent on the date of acceptance.

12. If the entity participating in any of the tender/bids is a private or public limited company, partnership firm or proprietary firm and any of the Directors/Partners/Proprietor of such company is also a director of any other company or partner of a concern or a sole proprietor having established business with IAA and has outstanding dues payable to the Authority, the said entity shall not be allowed to participate in IAA Tender/bids.

Assistant Manager (IT)
Indian Aviation Academy
Vasant Kunj New Delhi

****

GENERAL TERMS & CONDITIONS OF THE CONTRACT

1. Purpose & Scope

1.1. This document sets out the terms & conditions be met in connection with the "**Design, Development, Launching, Maintenance and associated services of e-Internship portal**" as given in the notice inviting Tender/bid & Qualitative requirements as detailed in **Scope of Work/Qualitative Requirements/Technical specifications** of this tender/bid document.

1.2. The Successful bidder shall have to sign a contract agreement on Rs.100/- Non- Judicial stamp paper. Cost of the stamp paper shall be borne by the Successful bidder.

2. Compliance

2.1 The unconditional acceptance of all the terms & conditions of the NIT has to be uploaded through a letter. The format of the letter is attached at Annexure-I.

2.2 The submission of the tender/bid will imply acceptance of all the tender/bid condition by the bidder laid in tender/bid document including all the Annexure(s) & schedules to the tender/bid document.

2.3 The compliance to the terms & conditions should be supported by authenticated documentation wherever required.

2.4 Each page of the Bid and cuttings / corrections shall be duly signed with stamp by the bidder.

2.5 The submission of unconditional acceptance as described in Para 2.1 of General terms and Conditions is essential for the tender/bid evaluation. The failure to submit the unconditional acceptance statement in the said format shall result in the tender/bid being rejected.

3. Language and Currency

3.1 The bidder shall quote the rates in English language and international numerals. The rates shall be in whole numbers.

3.2 In the event of the order being awarded, the language of all services, manuals, instructions, technical documentation etc. provided for under this contract will be English.

3.3 The bidders should quote only in **Indian Rupees** and the bids in currencies other than Indian rupees shall not be accepted.

4. Standard Conditions

4.1 Standard printed conditions of the bidder to the offer, other than the conditions specified here, will not be acceptable.

4.2 All entries in the tender/bid shall either be typed or be in ink. Erasures shall render such tender/bids liable to summarily rejection. The bidder shall duly attest all corrections, cancellation and insertions.

43 Bidder's offers shall be with reference to section and clause numbers given in the tender/bid schedules.

44 In case of any ambiguity between details given in NIT and Tender/bid, details given in Tender/bid shall be considered as correct.

5. Earnest Money Deposit (EMD)

5.1. **Earnest Money Deposit (**EMD) of the Value/Amount as mentioned in **CRITICAL DATA SHEET** shall be accepted **offline only** in the form of Demand Draft Drawn in favour of **Indian Aviation Academy (NIAMAR Society)** payable at **New Delhi** from a nationalized or any scheduled bank (**but not from co-operative or Gramin bank**).

5.2. Scanned copy of EMD DD should be uploaded in **fee folder (Envelope-1).**

5.3. The original Demand Draft against EMD should be posted/couriered/given in person to the concerned officials latest as specified in the Tender/bid Document.

5.4. The bid of the bidder, who fails to submit the original DD towards Tender/bid Fee & EMD before the stipulated time, shall be rejected out-rightly.

5.5. The details of Demand Draft, physically sent, should tally with the details available in the scanned copy and the data entered during bid submission time.

5.6. The EMD of all Unsuccessful bidders will be returned only after the opening of Financial Bid. No interest shall be payable on the Earnest Money Deposit.

5.7. The EMD of successful bidder will be released after submission of Security Deposit/PBG/ePBG of percentage (%) of the contract value as per GeM BID Document.

6. Time Schedule:

The provisioning of the Internship Portal & User acceptance test (UAT) shall be completed within **60 days** from award of work. In case of any functional & operational anomalies as stipulated in **Clause no. 9 of General terms and Conditions**, the final user acceptance test (FUAT) shall also be completed within aforementioned 60 days from award of work after which the **Clause no. 10 of General terms and Conditions**, '**Compensation for Delay**' shall be applicable.

7. Effective Date of Contract:

The start of contract period (Date of commencement of work) shall be counted from the Date of completion of User Acceptance Test (UAT) and/or Final User Acceptance Test (FUAT) i.e. post development of Internship portal.

8. Contract period:

Contract duration for this work/service shall be for two (02) year w.e.f. Effective date of Contract as mentioned in clause no: 7 above.

Subject to satisfactory services rendered during two (02) years of contract and on mutual consent between bidder and IAA, the contract period may be extended further for a maximum of one year on same rates, terms and conditions, provided a new agreement shall be signed for extended year.

9. **User Acceptance Test (UAT) & Final User Acceptance Test (FUAT):** The User Acceptance Tests for the Internship portal will be carried out at Indian Aviation Academy. After successful implementation of the system/service by the vendor, it will be the responsibility of the vendor to submit the 'USER ACCEPTANCE TEST DOCUMENT' for conducting the post implementation user acceptance test. The USER ACCEPTANCE TEST DOCUMENT, submitted by the successful bidder should be drafted in line with the standard practices followed in the industry & Qualitative requirements mentioned in Scope of Work/Qualitative Requirements/Technical Specifications of tender document. The USER ACCEPTANCE TEST DOCUMENT necessarily includes following tests:

A. Functional Tests
B. Operational Tests
C. Any other tests/evaluation criteria that IAA may specify

The draft copy of USER ACCEPTANCE TEST DOCUMENT should be made available to Project Manager, IAA for approval from competent authority not later than 15 days from award of work. The draft USER ACCEPTANCE TEST DOCUMENT upon approval by IAA shall become the document for acceptance of system/service. IAA reserves the right to add additional test(s) before or during UAT.

IAA UAT Team may witness system anomalies while performing User Acceptance Test.

Such anomalies shall be classified into following three categories:

Critical category anomalies: Critical Category Anomalies are defined as anomalies having operational impact on the basic & advance functionalities of the system/service.

Medium category anomalies: Medium category anomalies are defined as anomalies related to functionalities requiring minor software customization & user required modification which do not have direct impact on basic functionalities of the system/services.

Low category anomalies: Low category anomalies are defined as anomalies related to User interfaces and are of Low operational impact.

The above Category of failures shall be mutually agreed between successful bidder and IAA UAT team. Successful bidder has to resolve all the critical category failures, including as many as other type of failures (Medium and Low categories) after completion of UAT within the aforementioned timeline of 60 days from award of work. The resolution of these anomalies by successful bidder & corresponding verification tests by IAA shall be termed as Final user acceptance test (FUAT).

On successful testing of System anomalies as defined above, the Final UAT (FUAT) shall be treated as complete. System acceptance certificate will be issued by the IAA on the satisfactory report of a UAT team as Constituted by the Director, IAA for this purpose.

Warranty / Design and Development mode: Support of customization of the accepted system shall be available for 1 year from the date of initial acceptance without any additional cost.

10. Compensation for Delay

10.1. Time is the essence of the Contract.

10.2. If the successful bidder fails to complete the FUAT within time fixed under the contract, he shall pay to the IAA without prejudge to any other rights or remedy as may be available to the purchaser, an agreed compensation amount calculated @ 0.5 % of the total value of the contract per week subject to a maximum value equal to the value of the Performance Bank Guarantee.

10.3. The amount of compensation for delay and waiver of compensation for delay in case of justified reasons shall be decided at the discretion of Accepting Authority and the same shall be final and binding on the contractor. Force majeure reasons and any other reasons beyond control of the contractor shall be considered as justified reasons. The amount of compensation may be adjusted or set off against any sum payable to the contractor under this or any other contract with IAA.

10.4. Format for applying extension of time should be as per Annexure-VIII) of the tender/bid document.

10.5. Appeal for waiver of compensation for delay with due justification shall be decided as per the provisions of the Delegation of Powers (DOP) of Indian Aviation Academy. The decision of the competent authority on appeal shall be final and binding on the contractor**.**

11. Payment terms: No advance payment shall be paid by IAA.

(a) One time cost: 40% of the total cost will be paid as per Schedule of Quantities after the successful completion of acceptance test. This amount shall be released by IAA for Design, development & launching cost as per the Schedule of Quantities/BOQ upon successful Final User acceptance Test (UAT/FUAT

whichever is applicable) & after issuance of System Acceptance Certificate by IAA. Payment shall be released against the bill raised, as mentioned above by the successful bidder.

(b) Recurring cost: Rest 60% of the total quoted amount shall be released in eight (08) equal parts as mentioned below:

7.5% of the total cost as per Schedule of Quantities will be paid quarterly in equal installment for eight quarter for the cost of hosting, maintenance and associated services and first quarterly payment will be made after three months from the final user acceptance test.

(c) Variable cost in % age: 8.5% of the quarterly charges will be paid additionally for the usage charges for every additional users in the multiples of 200 and/or every additional certificates in the multiples of 2000 will be paid whichever is higher.

(d) In addition, any statutory taxes & TDS if applicable at the time of payment, as per prevailing Government norms shall also be deducted/paid.

(e) In case of extension of contract in subsequent year, the payment shall be released in four equal parts at the end of every quarter.

12. Performance Bank Guarantee/ Security Deposit

12.1. The successful bidder has to deposit percentage (%) of the contract value mentioned in GeM Bid Document as Security Deposit with IAA, in favour of IAA New Delhi, in the form of an irrevocable and unconditional bank guarantee on a Nationalized / Scheduled Bank within 30 days from the date of award of work and it should remain valid for a period of 90 (ninety) days beyond the date of completion of all contractual obligations of the successful bidder.

12.2. In case the successful bidder fails to submit the PBG within stipulated period, interest at 12% p.a. on Performance Guarantee amount would be levied (non- refundable) for delayed period of submission and shall be deducted from the first bill payable to the Contractor. It shall be lawful for the Procuring Entity at its discretion to annul the award and enforce Bid Securing Declaration, besides taking any other administrative punitive action like debarring from the future procurements.

12.3. In case, successful bidder fails to submit performance bank guarantee within 60 days from date of issue of work order, IAA reserve the right to forfeit EMD and cancel the order.

12.4. The Performance Security will be forfeited and credited to the accounts of IAA in the event of a breach of contract by the contractor. It should be refunded to the contractor without interest after he duly performs and completes the contract in all respects but not later than 90(ninety) days from date of completion of all such obligations.

12.5. Performance Bank Guarantee shall be made by the successful bidder as per proforma given in Annexure-VII of the tender/bid document.

13. SERVICE LEVEL AGREEMENT (SLA):

13.1. WARRANTY/SERVICES:

13.2.1. The vendor should provide post-implementation on-call support 9 AM to 5 PM for all functions and features of Internship portal to end users.

13.2.2. If the resolution is not provided through on-call/ online support within 24 hours, then onsite support & resolution must be provided within next 48 hours.

13.2.3. If the vendor is providing any hardware terminal on-site for any particular function for a cloud-based Internship environment, then the hardware support should also be provided by the vendor. The vendor should provide the support team structure and the roles and responsibilities of the support team member

13.2.4. The vendor should provide a complaint escalation matrix/ procedure.

13.2.5. The contractor/vendor shall be responsible for any damage, resulting from his negligence to existing fixtures and will restore, replace or repair any such damage to the complete satisfaction of the Project Manager. The contractor is also fully responsible for any breakage or damage to the property of IAA. Decision of Project Manager for recovery on this account shall be binding on the contractor and such amounts shall be adjusted from his bill.

13.2. PENALTY CLAUSE:

13.1.1. During the Contract period, penalty will be applicable & imposed in case of non- availability of Internship portal and associated services to the intended users.

13.1.2. Calculation of penalty amount shall be done as per the below-mentioned criteria.

UPTIME:

• The Internship system has to be up for at least 99.9% of the time as per the scope of work. The Internship portal is deemed to be up if the users are able to log into the system and are able to fully execute all the functionalities of the system.

• The uptime shall be computed on a monthly basis.

- **Uptime:** The percentage uptime shall be calculated on monthly basis as follows:

Availability % = (Total No. of Hours in month – Total Outage Hours in the month)/(Total No. of Hours in month) x 100

In case uptime falls below the guaranteed level i.e. 99.9%, IAA will impose penalty of 1% of the contract value for each percent below the guaranteed level, subject to the ceiling of 10% annually.

14. Correspondence

All correspondence would be done directly with the successful bidder and correspondence through agents will not be entertained.

15. Force Majeure:

15.1. IAA may grant an extension of time limit set for rectification of fault is delayed by force majeure beyond the contractor's control, subject to what is stated in the following sub paragraphs and to the procedures detailed their-in being followed.

15.2. Force Majeure is defined as an event of effect that cannot reasonably be anticipated such as acts of God (like earthquakes, flood, storms etc.), acts of states, the direct and indirect consequences of wars (declared or un-declared), hostilities, national emergencies, civil commotion and strikes (only those which exceed a duration of ten continuous days).

15.3. The successful bidder's right to an extension of the time limit for completion of the work in above-mentioned cases is subject to the following procedures:

16.3.1. That within 10 days after the occurrence of a case of force Majeure, the bidder informs the IAA in writing about the occurrence of Force Majeure Condition and that the Bidder considers himself entitled to an extension of the time limit. The contractor shall submit the application for extension of time.

16.3.2. That the contractor produces evidence of the date of occurrence and the duration of the force majeure in an adequate manner by means of documents drawn up by responsible authorities.

16.3.3. That the contractor proves that the said conditions have actually been interfered with the carrying out of the contract.

16.3.4. That the contractor proves that the delay occurred is not due to his own action or lack of action.

16.4. Apart from the extension of the time limit, force majeure does not entitle the successful bidder to any relaxation or to any compensation of damage or loss suffered.

17. Patents, Successful bidder's Liability & Compliance of Regulations

17.1. Successful bidder shall protect and fully indemnify the IAA from any claims for infringement of patents, copyright, trademark, license violation or the like.

17.2. Successful bidder shall also protect and fully indemnify the IAA from any claims from successful bidder's workmen/employees, their heirs, dependents, representatives etc. or from any person(s) or bodies/ companies etc. for any act of commission or omission while executing the order.

17.3. Successful bidder shall be responsible for compliance with all requirements under the laws and shall protect and indemnify completely the IAA from any claims/penalties arising out of any infringements and indemnify completely the IAA from any claims/penalties arising out of any infringements.

18. Settlement of Disputes

18.1. If a dispute of any kind whatsoever arises between the IAA and the Contractor in connection with, or arising out of the Contract or the execution of the works, whether during the execution of the Works or after their completion and whether before or after repudiation or after termination of the contract, including any disagreement by either party with any action, inaction, opinion, instruction, determination, certificate or valuation of the Project Leader or his nominee, the matter in dispute shall, in first place be referred to the Director, IAA who shall act as the conciliator on the matter. The disputes will firstly be settled by the Conciliator, failing which any party may invoke arbitration clause.

18.2. Unless the Contract has already been repudiated or terminated or frustrated the Contractor shall in every case, continue to proceed with the works with all due diligence and the Contractor and IAA shall give effect forthwith to every decision of the Project Leader or his nominee unless and until the same shall be revised, as hereinafter provided, by the Conciliator or in an Arbitral Award.

19. Arbitration and Law

19.1. Except where otherwise provided for in the contract, all questions and disputes relating to the provisions of this contract shall be settled under the Rules of Indian Arbitration and Conciliation Act, 1996, within thirty (30) days (or such longer period as may be mutually agreed upon from the date that either party notifies in writing that such dispute or disagreement exists. The Director, IAA shall appoint the single Arbitrator for settlement of any dispute with regard to this contract. The venue of Arbitration shall be in New Delhi, India. The arbitration resolution shall be final and binding upon the parties and judgment may be entered thereon, upon the application of either party, by any court having jurisdiction.

19.2. Indian laws shall govern this contract.

20. TERMINATION FOR DEFAULT & RISK PURCHASE

20.1. The IAA may, without prejudice to any other remedy for breach of contract, by written notice of default, sent to the Contractor, terminate this Contract:

20.2. If the Contractor fails to fulfill the tendered obligations & terms and conditions within the time period(s) specified in the Contract.

20.3. If the Contractor, in either of the above circumstances, does not remedy his failure within a period of 30 days (or such longer period as IAA may authorize in writing) after receipt of the default notice from IAA.

20.4. As a penalty to the Contractor, IAA shall forfeit the Performance Security. IAA in such case shall pay for the assessed value of the executed work that can be used. No payment shall be made for the efforts put in by the Contractor in case the same are of no value to IAA. The balance unfinished work of the project will be got done by fresh tendering on Contractor's risk and that extra expenditure will be recovered.

SPECIAL CONDITIONS OF THE CONTRACT

The following special conditions shall be read in conjunction with IAA General Conditions of contract. If there are any provisions in the special conditions of contract, which are at variance with the provisions of General Conditions of Contract of IAA, then the provisions in these special conditions shall take precedence.

1. GENERAL

i. Special conditions of Contract shall be read in conjunction with General Conditions of Contract, Qualitative Requirement and any other documents forming part of this contract wherever the context so requires.

ii. Notwithstanding the sub-division of the documents into these separate sections and volume every part of each shall be deemed to be supplementary to and complementary of every other part and shall be read with and into the CONTRACT so far as it may be practicable to do so.

iii. Where any portion of the General Condition of Contract is at variance with any provisions of the Special Conditions of Contract, the provisions of the Special Conditions of Contract shall be deemed to over-ride the provisions of the General Conditions of Contract.

2. SCOPE OF WORK

The scope of work in this Tender/bid covers "**Design, Development, Launching, Maintenance and associated services of e-Internship portal**". It includes all software, hardware, materials, workforce, tools, supervision etc. required for provision of services as specified in Scope of Work/Technical Specifications/Qualitative Requirements. The details of scope of work is specified in Scope of Work/Technical Specifications/Qualitative Requirements.

2.1. The bidder or its authorized representative is aware of all technical specifications and operational requirements of the tendered services.

2.2. The successful bidder shall ensure that meeting all statuary obligations, licensing requirements and any personal compensation arising due to this provisioning & launching of Internship portal system, hosting, maintenance & associated services are sole responsibility of successful bidder.

2.3. The successful bidder will ensure immunity to IAA from any point arising due to patent / copy right rules.

3. Support Services

3.1 The vendor should provide post-implementation on-call support 9 AM to 5 PM for all functions and features of Internship portal to end users.

3.2 If the resolution is not provided through on-call/ online support within 24 hours, then onsite support & resolution must be provided within next 48 hours.

3.3 If the vendor is providing any hardware terminal on-site for any particular function for a cloud-based Internship environment, then the hardware support should also be provided by the vendor. The vendor should provide the support team structure and the roles and responsibilities of the support team member

3.4 The vendor should provide a complaint escalation matrix/ procedure.

3.5 The contractor shall be responsible for any damage, resulting from his negligence to existing fixtures and will restore, replace or repair any such damage to the complete satisfaction of the Project Manager. The contractor is also fully responsible for any breakage or damage to the property of IAA. Project Manager decision for recovery on this account shall be binding on the contractor and such amounts shall be adjusted from his bill.

4. Training of Users

4.1. The vendor should provide at least one onsite training of 3 to 5 days about course administration through Internship Portal.

4.2. The vendor should use multimedia training aids such as pdf, ppt, doc, xls etc. for functional and technical training materials for all the users of Internship application.

4.3. The vendor is expected to maintain, edit and update all training content of Internship portal in sync with changes made in the Internship solution throughout the contract period.

5. CONTRACT AGREEMENT

5.1. The contract agreement shall be executed on a non-judicial stamp paper of value Rs.100/- and cost of the stamp paper shall be borne by the Contractor.

5.2. The tender's terms & conditions including the letters of clarifications between the contractor and the IAA prior to the award of contract shall form a part of the Contract Agreement to the extent they have been accepted by IAA.

5.3. **Confidentiality & Non-Disclosure Agreement:** After the award of work, the successful bidder has to enter with IAA into a Non-disclosure Agreement which shall be complied by the successful bidder for non-disclosing of the proprietary course material of IAA to any other person/company, except the intended users of IAA & also limit disclosure of this proprietary information to their directors, officers, employees, agents or representatives (collectively "Representatives") who have a need to know such Proprietary Information for execution of the awarded work.

This agreement shall be executed between authorized representative of Director (IAA) & successful bidder on a Rs 100 Non-Judicial stamp paper. Cost of stamp paper is to be borne by successful bidder

6. BYE-LAWS

6.1. The contractor shall comply with all bye-laws and regulations of local and statutory authorities having jurisdiction over the works and shall be responsible for payment of all fees and other charges and for giving and receiving of all necessary notices and keeping the Project Manager, informed of the said compliance with the bye-laws, payments made, notices issued and received.

6.2. The contractor shall indemnify the IAA against all claims in respect of patent rights, design, trademarks of name or other protected rights in respect of any plant, machine, work or materials used for or in connection with the work or temporary works and from and against all claims, demands proceedings, cost, charges and expenses whatsoever in respect of or in relation thereto. The contractor shall defend all actions arising from such claims and shall himself pay all royalties license fees, damages, costs and charges of all and every sort that may be legally incurred in respect thereto.

6.3. Contractor has to comply with the provisions of Contract Labour (Regulations and Abolition) Act 1970 and Contract Labour (Regulations and Abolition) Central Rules 1971 and Minimum Wages Act & Rules thereof Central and State Governments with up to date amendments.

7 Exit Management Plan

7.1 In any of the circumstances where:
(i) End of the contract period
(ii) Bankruptcy of the successful bidder
(iii) Violates the terms and conditions
(iv) IAA on its discretion decides to remove the contractor by giving a notice period.
(v) Or any other case where the contract is getting closed or completed.

In all of the above circumstances, bidder has to follow the Exit Management Plan (Annexure- VI) as described below:
a) Provide complete integrity of user data, course content and shall return back all the user information, course content to IAA.
b) All course related information has to be given back to IAA and no information in any aspect has to be withheld by the bidder before leaving the contract.
c) Shall have to clear all database, cache containing any information about IAA and cannot further host any of the IAA logo, name, image, course in any form on any platform whatsoever.
d) Duplicity/Copying or using of Course Content for any other purpose provided by IAA in any other form is strictly prohibited.

Violating of any of the above conditions shall be treated as breach of personal information and further actions shall be taken as deemed fit as per Information Technology Act.

****

Scope of Work/Qualitative Requirements/Technical Specifications

1. Introduction:

As part of an initiative to promote awareness about the aviation industry among the youth, Airports Authority of India (AAI) desires to collaborate with educational institutions and provide first-hand exposure to the students on the working of Civil Aviation sector. For the same, three different learning opportunities are being offered to students:

1.1. **Familiarization programmes (FP)**, spanning 2-5 days round the year, offering flexibility and in-depth experience at Airports covering Air Traffic Management, Communication, Navigation & Surveillance, Civil and Electrical Engineering, Airport Operations, and Information Technology. Further it is referred to as FP.

1.2. **Internship programmes (IP)** for 4-20 weeks during summer and winter, which is tailored to the academic calendar for summer and winter sessions. Programmes cover diverse disciplines like Architecture, Airport Operations, Engineering, Finance, HR, IT, Law etc. Further it is referred to as IP.

1.3. **Being part of Project Implementation at Airports (Observe implementation and Learn)**, witnessing in-progress development, expansion works, and project execution spanning 2-5 days. Further it is referred to as BPI.

All the above three schemes will be administered through portal by Indian Aviation Academy (IAA) on behalf of AAI and further it is referred to as buyer.

2. Services sought.

2.1. Managing end-to-end implementation of Internship Program of AAI comprising of:

2.1.1. An online portal to manage internship scheme through which, Educational Institutions (pan-India) can view, search, and apply for the programs as highlighted in 1.1-1.3 above i.e. FP, IP and BPI.

2.1.2. Extensive outreach of the Internship program among educational institutions to generate interest as per clause 3.2 of Scope of Work.

3. Workflow

3.1. **Registration**

3.1.1. The entire portal and its content shall be accessible to any visitor in an organized manner with search options and effective filter options to find the information about all the three programs (FP, IP & BPI), discipline wise and city wise. This information shall include the total slots, availed and open slots for a particular discipline, particular program, and city.

3.1.2. When any visitor tries to apply for a particular program, it shall prompt a suitable message desired by the buyer. This message shall be configurable by the buyer.

3.1.3. Apart from standard navigation menus / buttons, download menu/button shall be available where the documents meant for sharing with the users shall be available. Provision for uploading these documents on standard file formats by user admin shall be available.

3.1.4. Contact menu / button in home tab shall lead to the email id of help support.

3.1.5. When any willing institute tries to register, they will be prompted to select their institute from the populated list in the portal. If their institute name is available, they will start applying for the registration. If their institute name is not found, they will send mail to the support desk.

3.1.6. Once registration request is received user admin will verify the MOU, college profile and other documents, verify and validate and map the domains of FP, IP, and BPI suitable to the institute and enable the account.

3.1.7. Once the college user account is enabled, they will be able to select and apply for FP, IP and BPI as per their choice.

3.1.8. AICTE/UGC approved educational institutions with valid email id of registrar / Training & Placement Officer (TPO) or any other colleges and universities as desired by the buyer will be allowed to register. For the same, the list of all AICTE/UGC approved colleges to be populated by the vendor on the portal for the colleges to select and register. Further in addition, all the list of colleges and universities given by the buyer also need to be populated. The populated list shall have the name and address of the institutes.

3.1.9. Signing a Memorandum of Understanding (MoU) shall be a pre-requisite for registration. Copy of the MOU or its update shall be uploadable by the buyer as and when needed and the same shall be accessible by the interested institutes with immediate effect. Also, the signed and scanned copy of the MOU shall be up loadable by the institute along with other documents while registering. All standard file formats shall be supported.

3.1.10. During registration process, educational institutions shall be able to select the courses for which familiarization / internship is sought as per the program offered by them. The master list of courses from which the graphics user interface will be made available to the users shall be updatable by the buyer.

3.1.11. Provision of email and phone number verification for educational institutions to be made in order to avoid duplicate entries.

3.1.12. After registration, authorization of account to be done by user admin after checking credentials and MoU.

3.1.13. Educational institutions profile shall comprise of editable fields like name and contact details of registrar / TPO.

3.1.14. There shall be four levels of user logins namely (1) Super admin (2) user admin (3) Station user and (4) College user.

3.1.15. Super User Admin shall have complete rights for all the user administration. User admin will have rights for all the station and college users' administrations. All the users will be able to modify, add, delete their own profile data, and other data they upload in the system.

3.2. **Outreach**

3.2.1. User admin should be able to bulk upload and publish details of upcoming IPs & FPs, along with the available slot and start date on the portal. Also, provision for revision (Modify/Add/Delete) to be made. And as and when required individual updates also will be made on each slots pertaining to airport and subject domain.

3.2.2. In case of BPI(Para 1.3), Station Admin should be able to send notification (email / WhatsApp) to nearby institutions with details on how to avail the opportunity. Customized email content to be developed for the same.

3.2.3. Whenever IPs & FPs are published, updated (addition, deletion & modification) email & WhatsApp notification should be sent to all registered educational institutions. For BPI(PARA 1.3) , notification to be sent to institutions in the vicinity. At the same time, the opportunity shall be visible on Dashboard of the educational institutions.

3.2.4. For providing the update as per para above to each college minimum of five email ids and five mobile numbers will be configured. And these configuration shall be editable by the respective college user as well as user admin.

3.2.5. The internship opportunity shall clearly indicate date of closing, beyond which the window to apply shall close.

3.2.6. The home page of the portal should show live Internship programs to create interest among students.

3.2.7. Social Media promotion of the IPs & FPs should be done through channels like LinkedIn, Facebook, X (Twitter) etc. All expenses should be born by successful bidder. Contents for uploading into these accounts will be shared by the buyer as and when needed. All these applications shall be integrated into the portal.

3.2.8. Provision of email reminders to be made for remaining slots and deadlines.

3.2.9. Dedicated Customer Service Helpdesk (9 am – 5 pm), FAQ page for educational institutions & students to be made available for resolution of technical queries. Detailed step-by-step manual to be made available in downloadable format.

3.2.10. The Outreach activities shall be carried out to bring at least 100 more colleges (measured by increase in user login) every year over and above number of colleges available during the final user acceptance test or in the previous year whichever is higher. The date of user acceptance test will be considered as a beginning of the contract year.

3.3. **Application & Selection**

3.3.1. Eligible institutions should be able to submit student applications for the Internship program through portal login. While applying for internship, eligibility criteria to be matched. Unique ID to be created for each student whose application is being uploaded.

3.3.2. While uploading student data, details like Name, Gender, Date of Birth, Photo id Proof, Photo id number, mobile number URL, etc shall be mandatory fields. Provision for uploading identity documents of students for security pass to be kept. These requirements shall be adaptable by user admin.

3.3.3. User admin should be able to view Station & Department-wise applications received and approve students on First-Come-First-Served basis.

3.3.4. After approval, an email / WhatsApp communication to be sent to the institute containing the student permission letter(s) and joining instructions; with a copy to the concerned Station.

3.3.5. The institutes should be able to view and download permission letters issued from Dashboard.

3.3.6. Available slots to change on a real-time basis depending upon the approvals granted.

3.4. **Training, Certification & Feedback**

3.4.1. Student details shall be highlighted in the Dashboard of Station admin. Station admin shall mark the attendance of interns on the portal on Day 1 of reporting, which shall be reflected in User Admin Dashboard (Station-wise Permitted Vs Reported)

3.4.2. In case of IP, Project Report (pdf format) shall be submitted by the student to respective HoD with a copy to Station admin, who shall upload it on the portal

3.4.3. After marking of attendance during the internship period and uploading Project Report, a verifiable certificate (with a QR code) to be generated and emailed to the student as well as the institution

3.4.4. Provision for providing feedback regarding IP to be made

4. Data Management & Reporting

4.1. All data shall be hosted on cloud-based server system

4.2. Data archiving to be taken periodically on cloud

4.3. Customized Reports to be made available in MS Excel or CSV format to User Admin and Station Admins

4.4. Provision shall be made for uploading of content in PDF, MS Word, MS Excel and MS PowerPoint format

4.5. User admin / Station-admin / Educational Institutions shall be able to view customized Dashboard for monitoring progress (Station-wise, Program-wise, Month-wise) and download / print reports

5. General Specifications

5.1. Entire Internship program (listed in 1.1, 1.2 &1.3 of scope of work) to be administered through a portal (to be able run on Google Chrome, Microsoft Edge, Safari, Mozilla Firefox, etc) and through all well-known OS platforms (Ubuntu, Windows, Macintosh, Android, iOS, etc.)

5.2. Entire internship program (listed in 1.1, 1.2 &1.3 of scope of work) along with latest update shall be available in android app and it should be accessible to any public.

5.3. Entire administration of the Internship scheme will be done through the portal, including web-generated communication through an inbuilt Email gateway or a Mail server

5.4. The portal / App shall comply with all cybersecurity measures mandated by GoI

5.5. No third-party access of student particulars of any other internship data to be given.

5.6. User interface should have simple login/logout procedures with validation checks and password reset options, navigation menu, visually clean and uncluttered web page, and GUI. Post selection of vendor, requirements will be given in detail and should be customizable for a period of one year.

5.7. The system which provides Software as a Service (SaaS) should be available 24x7 with an uptime of 99.9% or conforming to the provisions laid in SLA. The planned downtime needs to be communicated 30 days prior to the schedule.

6. Scalability and Customization

6.1. System shall be configurable with the existing as well as new email ids for communicating with educational institutions, User admin and Station admin

6.2. Apart from the User Admin, there shall be adequate resource to have minimum 600 user logins to begin with and gradually to increase to minimum of 1,000 user logins in two years. At the same time, system shall be capable of having 2,000 user logins as and when required.

6.3. System shall be capable of generating and storing certificates of minimum 6,000 certificates to begin with, gradually increasing to over 10,000 certificates per year over and above the previously stored certificates. At the same time, system shall be scalable to store 20,000 certificates per year as and when needed.

6.4. Provision for generation of customized certificates for trainings other than IP to be made available.

7. Contractual terms and conditions

7.1. The contract shall be valid for two years, extendable by one year.

8. Development & Maintenance of Internship portal

8.1. Successful bidder will design & develop Internship portal as mentioned in scope of work and further provide maintenance services for Internship portal post development of Internship portal till end of the contract. Maintenance services of Internship portal shall commence post development of Internship portal and the support services shall be put in place by vendor for maintenance services of Internship portal till end of the contract and support services shall meet the performance levels of Service Level Agreement (SLA).

8.2. Security audit of Internship portal: Get Internship portal audited yearly. It is vendor's responsibility to rectify the issues and provide the security audit certificate from a CERT-In empaneled agency and also ensure strict compliance as per cyber security guidelines mentioned in Annexure-IX. Checklist for Comprehensive Security Audit is enclosed at Annexure-X for strict compliance.

8.3. SSL Certificates: Procure and deploy wildcard SSL certificate on server for maintaining the website through https protocol and also ensure strict compliance as per cyber security guidelines mentioned in **Annexure-IX.** Checklist for Comprehensive Security Audit is enclosed at **Annexure-X** for strict compliance.

8.4. Quality certification of Internship portal: Normally the Internship portal related quality certification provided by Standardization Testing and Quality Certification (STQC)/ designated agency is valid for 3 years. These payments required for such certification is made by the bidder for certification and also ensure strict compliance as per cyber security guidelines mentioned in Annexure-IX. Checklist for Comprehensive Security Audit is enclosed at **Annexure-X** for strict compliance. It is required that corrections/rectification of errors raised by STQC/any other empaneled agency during annual surveillance is done to maintain GIGW compliance as per Govt guidelines. The vendor is required to address and resolve the errors/ non-conformities if any rose during the audit/annual surveillance activities by any government agencies/ AAI/ IAA.

8.5. Maintenance of Internship portal shall include following items, but not limited to

8.5.1. Creation, updating & Maintenance & backup of related Internship portal/ web page/ user login**.**

8.5.2. Improve logic & design whenever required to enhance performance of website**.**

8.5.3. All procurement and licenses shall be carried out in the name of buyer and associated costs will be borne by the bidder.

9. Functional and other qualitative requirements.

Following are detailed explanation of requirements highlighted in the above paras on various functional and qualitative requirements.

9.1. User Interface (UI) Design

9.1.1. The internship portal shall meet the following design parameters and qualitative requirements so that the portal not only looks visually appealing but also provides a seamless and satisfying user experience.

9.1.2. Navigation shall allow users to easily find the information they need, with clear hierarchy of menus, categories, and navigation elements and consistent navigation across different sections of the portal.

9.1.3. Design shall have aesthetic appeal with visually appealing layouts, colours, typography, and imagery. Shall have branding elements that reflect the portal's identity and purpose. Shall have enhance readability and focus attention on key elements.

9.1.4. Portal shall meet the accessibility standards mentioned in the tender document. Design shall meet the responsiveness requirements to ensure the portal functions well across various devices and screen sizes. Layout and other elements shall adapt to different resolutions and orientations. Portal shall have all engaging interactive elements such as buttons, forms, sliders, and animations. There shall

be feedback mechanism to provide visual cues and confirmations for user actions.

9.1.5. Consistent design patterns and visual elements shall be implemented throughout the portal and consistency shall be maintained across different pages and sections.

9.1.6. Content Presentation shall be Clear and concise with appropriate headings, paragraphs, and formatting. Multimedia elements (images, short videos, audio) shall be used to enhance content and engage users.

9.1.7. Feedback and Error Handling systems should be in place to notify users of successful actions, errors, or validation issues, with error messages with suggestions for resolving issues and continuing with the task. Also, necessary visual indications shall be used to highlight active states, hover effects, and changes in interface elements.

9.1.8. User Feedback Integration shall be made to provide feedback, such as surveys, contact forms, or rating systems.

9.2. User Experience (UX) Design

The internship portal shall meet the following design parameters and qualitative requirements so that the portal effectively meets the needs and expectations of its users or audiences i.e. training and placement officers, registrars, deans and VCs of colleges, universities, and other institutes.

9.2.1. User Research: Bidder shall Conduct user research to understand the needs, goals, and behaviours of the target audiences if needed shall gather insights through methods such as interviews, surveys, user testing, and analytics.

9.2.2. Information Architecture: Content and features shall be organized in a logical and intuitive manner, in such a way that users shall be able to access information and complete tasks efficiently.

9.2.3. Usability: Design of the website shall be easy to learn, efficient to use and error-tolerant. During user acceptance test, usability issues will be tested, and design improvements will be brought up based on the observation.

9.2.4. Visual design: Create a visually appealing and cohesive design that aligns with the brand identity and user expectations. Visual hierarchy, typography, colour, and imagery to guide users' attention and enhance comprehension.

9.2.5. Consistency: Maintain consistency in design elements, terminology, and interaction patterns across different parts of the portal. Ensure a seamless experience as users navigate between pages and sections.

9.2.6. Performance: Performance optimization shall be done to ensure smooth responsiveness. Prioritize content and features based on their importance and frequency of use to enhance perceived performance.

9.3. Backend

9.3.1. Scalability: Design the backend architecture to scale horizontally or vertically to accommodate growing user traffic and data volumes. Implement load balancing, caching mechanisms, and distributed systems to handle increased demand.

9.3.2. Performance monitoring: Optimize database queries, and server-side code to minimize response times and ensure a smooth user experience. Use performance monitoring tools to identify bottlenecks and optimize resource utilization.

9.3.3. Reliability: Portal shall have in built fault-tolerance and shall recover gracefully

from failures without disrupting the user experience. Data loss shall be prevented with proper backup and disaster recovery strategies.

9.3.4. Data Management: Design efficient data models and database schemas to store, retrieve, and download data effectively.

9.3.5. Concurrency and Threading: Concurrent requests shall be handled efficiently to prevent bottlenecks and ensure responsiveness under heavy load. Concurrency control mechanisms shall be made to manage shared resources and avoid data corruption.

9.4. Front end

9.4.1. Cross-Browser Compatibility: In addition to the UI & UX as described earlier, frontend codes shall be tested and debugged across multiple browsers and browser versions to identify and address compatibility issues.

9.5. Authentication and Authorization

9.5.1. Verification of the identity of users attempting to access the portal shall be done by unique credentials such as usernames, email addresses, or mobile numbers. Authentication shall be done based on passwords and OTP.

9.5.2. Role based access control shall be defined for the super user admin, user admin, station admin and college users that determine what actions different categories of users are allowed to perform within the portal. Granular permissions to control access to specific features, functions, or resources based on user roles and responsibilities shall be implemented based on buyers' feedback. Dynamic adjustment of permissions shall be possible based on changing user roles, group memberships, contextual factors or as per the buyers need.

9.5.3. User sessions shall be managed securely to maintain authentication state and track user interactions during their session. Session timeout mechanisms shall be implemented to automatically log out inactive users after a defined period to mitigate the risk of unauthorized access.

9.5.4. Strong password policies shall be enforced such as minimum length, complexity requirements, and expiration periods to enhance security. Passwords shall be stored securely to protect against unauthorized access in the event of a data breach. Secure mechanisms shall be implemented for users to recover or reset their passwords in case they forget them, such as email-based password reset workflows.

9.5.5. Audit logs shall be maintained of authentication and authorization events to track user activity, detect suspicious behaviour, and facilitate forensic analysis in case of security incidents. Authentication and authorization processes shall be monitored in real-time to identify anomalies, unauthorized access attempts, or security threats.

9.5.6. Sensitive data exchanged during authentication and authorization processes shall be encrypted using strong encryption algorithms to prevent eavesdropping and tampering. Secured communication protocols shall be used to establish encrypted connections between clients and servers for authentication and data transmission.

9.6. Search Functionality

9.6.1. Search results shall be accurate and relevant to the user's query by implementing robust keyword matching algorithms. Ranking algorithms shall be used to prioritize search results based on factors such as relevance, popularity, recency, and user engagement.

9.6.2. Search filters and features shall be provided to allow users to refine their search results based on criteria such as discipline, city, program, and other relevant attributes as desired by the buyer. Dynamic filtering mechanism shall be in place to update search results in real-time as users apply or remove filters.

9.6.3. Autocomplete suggestions shall be implemented as users type their search queries to help them quickly find relevant keywords and phrases. Queries shall be suggested based on popular or trending search terms to guide users and improve their search experience.

9.6.4. Spell checking algorithms shall be implemented to detect and correct misspelled words in search queries, improving the likelihood of finding relevant results.

9.6.5. Intuitive search UI elements such as search bars, filters, and sorting options shall be implemented to make it easy for users to perform searches and refine results. Visual feedback, such as loading indicators or progress bars shall be implemented to indicate that the search is in progress and reassure users that their query is being processed.

9.6.6. Search results shall be displayed with relevant snippets or excerpts highlighting the matched keywords within the context of the content.

9.6.7. Ensure that the search functionality is responsive and optimized for mobile devices, with intuitive touch-friendly controls and layout adjustments.

9.7. Mobile Responsiveness

9.7.1. Webpage shall scale properly and adapts to different screen sizes and shall ensure that content adjusts dynamically based on the viewport size.

9.7.2. Contents shall be organized into columns and rows that reflow and rearrange themselves based on the device's screen size.

9.7.3. Images and media elements shall resize proportionally and shall not exceed the width of their containing elements.

9.7.4. Touch-friendly controls, buttons, and navigation elements that are easy to tap or swipe on touchscreens, with adequate spacing and sizing to prevent accidental clicks shall be implemented.

9.7.5. Legible fonts and font sizes that are readable on small screens, with appropriate line heights and letter spacing for optimal readability shall be adopted.

9.7.6. Mobile responsiveness of the portal across different mobile browsers (e.g., Chrome, Safari, Firefox) operating systems (e.g., iOS, Android) and devices (e.g., Tablet, mobile, laptop) shall be tested to ensure consistent rendering and functionality.

9.8. Data analytics

9.8.1. Wide range of data points including user interactions, traffic sources, demographics, and device types to gain a comprehensive understanding of user behaviours shall be collected in real-time, stored and shared with the buyer in .CSV format periodically once in a month.

9.8.2. Accuracy and integrity of collected data shall be ensured by implementing

validation checks and error handling mechanisms. Data also shall be validated to remove duplicates, and inconsistencies.

9.8.3. Interactive dashboards and visualizations that allow super user admin, user admin, station admin and college users to explore data intuitively and gain insights briefly. Custom reports and data exports tailored to stakeholder requirements as desired by the buyer shall be possible.

9.8.4. User engagement metrics, traffic sources and attribution, user segmentation and relevant metrics shall be captured and shared periodically for improvising the outreach strategies.

9.9. Scalability and Flexibility

9.9.1. The portal architecture shall be designed to scale horizontally by adding more servers, instances, or nodes to accommodate increased user traffic and data loads.

9.9.2. Vertical scalability shall be made by upgrading server resources (CPU, memory, storage) to handle growing workloads and resource demands.

9.9.3. The portal shall be designed with a modular architecture that allows for easy addition, removal, or modification of components and features, facilitating flexibility and adaptability.

9.9.4. Appropriate mechanism shall be adopted to break down applications into smaller and modular approach so that module or component can be modified and upgraded without affecting the entire portal.

9.10. User acceptance test (UAT)

9.10.1. Comprehensive test plan outlining testing objectives, scope, approach, resources, and timelines shall be proposed by the successful bidder at least 10 working days before the scheduled UAT. This shall include testing strategies for different aspects of the portal, including functional testing, performance testing, security testing, and usability testing.

9.10.2. Functional testing shall be done against the functional specifications to verify the portal meeting the specified requirements.

9.10.3. Usability testing, performance testing, compatibility testing, data analytics testing, and other requirements specified in the tender document will also be done as a part of UAT. The final test procedures and schedule and timeline will be approved by the buyer within 5 working days after the draft UAT procedure submitted by the successful bidder.

9.10.4. It is the responsibility of the successful bidder to demonstrate or provide the evidence of the portal functionality, performance and compliance of the requirements specified in the tender document to the buyer either through demonstration or through appropriate certified testing agency of government of India.

10. Scope of the work defined above are essential, however the successful bidder is expected to add additional values out of expertise and experience to meet the smooth administration of all the programs mentioned on para 1.1 to 1.3.

****

Annexure-A

CHECKLIST of Cover-I /(PQQ cum FEEs)

(To be uploaded by applicants along with tender/bid application in Envelope-I i.e. (Fee) Bid)
(Tender/Bid ID: GEM/2024/B/4926424)

Name of work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal"

Ref No.	Qualifying Criterion	Particulars	Enclosure check list 1.
1	**Envelope-I should consists of following details**		
a	Details of Tender/bid Fee (DD)	Self-attested copy of Bank DD – **Necessary document**. (Exemption certificate with supporting documents may be given in this stage if applicable)	**Tender/Bid Fee (DD)** (Enclosed / Not Enclosed)
b	Details of Earnest Money Deposit (EMD) (DD)	Self-attested copy of Bank DD- **Necessary document**. (Exemption certificate with supporting documents may be given in this stage if applicable)	**EMD Fee (DD)** (Enclosed / Not Enclosed)
c	Scanned copy of duly signed and Stamped Unconditional Acceptance of IAA's Tender/bid Conditions. (Performa given on **Annexure-I** of tender/bid document)	**Necessary document**	**Unconditional Acceptance Letter** (Enclosed / Not Enclosed)
d	Authorization letter/ power of attorney (If applicable)	**Necessary document**	**Authorization Letter/ Power of Attorney** (Enclosed / Not Enclosed)
e	Valid NSIC/MSME registration certificate issued by competent authority, in case of seeking for exemption for Tender/bid Fee and EMD by the NSIC/MSME registered firms.	**Necessary document**	**NSIC/MSME registration certificate** Enclosed / Not Enclosed

Envelope-II: - The Financial e-Bid through GeM portal:			
	Standard BOQ (.xls)	**Necessary document**	Enclosure of BOQ: Yes/No
	Note: BOQ must be uploaded by all bidders at the time of Financial e-bid opening (Envelope-II) only through GeM portal.		

DECLARATION

I (_____) hereby declare that the documents submitted / enclosed are true and correct. In case any document at any stage found fake / incorrect, action as deemed fit by IAA can be taken against me.

Place:
Date:

Signature
Authorized Signatory of the contractor/ Firm
(Signature with stamp)

****

Annexure-B

CHECKLIST of Cover–I/ (PQQ cum Technical)

(Pre-Qualifying cum Technical Proforma to be uploaded by applicants along with tender/bid Application in Envelope-I)

(Tender/Bid ID: GEM/2024/B/4926424)

Name of work: "Design, Development, Launching, Maintenance and associated services of e-Internship portal"

1	2	3	4
Ref No.	**Qualifying Criteria**	**Particulars**	**Enclosure Check List**
1	Name and Registered Office Address of the Firm / Contractor	**Name:** **Address:** **Ph. No. (Office):** **Mobile No.:** **Fax No.:** **E-mail ID:** **(Necessary documents)**	

2	Details of valid registration in appropriate class of CPWD / MES / P&T / RAILWAYS / STATE PWD / PSUs / Municipal Corporations & Development Authorities of Delhi, Mumbai, Chennai and Kolkata / Manufacturers (or) their Authorized Dealers (or) Agency specialized in similar nature of work and Registered with Registrar of Companies / Firms / Central Govt. / State Govt. entity in India.	Certificate of Incorporation or Registration should be valid & verified document as applicable on certificate (**Necessary document**)	**Copy of Registration Certificate/Certificate of Incorporation** (Enclosed / Not Enclosed)
3	Valid Permanent Account Number (PAN) from Income Tax and GST Registration Certificate.	PAN Card & GST registration certificate should be valid & verified documents (**Necessary document**)	**PAN Card & GST Registration Certificate** (Copy Enclosed / Not Enclosed)
4	Digitally / signed Tender/bid Document	(**Necessary document**)	**Tender/bid Document** (Enclosed / Not Enclosed)
	Certificate from clients of having satisfactorily Completed similar works.	Details of the **Three/Two/One works as applicable** (**Necessary document**)	**Copy of work completion certificates as applicable** (Enclosed / Not Enclosed)

5	a) Three works of 40 % OR b) Two works of 50% OR c) One work of 80% of estimated amount in single contract of similar nature during last 7 years ending on last date or extended date for submission of bid, in India	**1.Client:** **Name of Work:** **Order No. & Date:** **Cost:** **Date of completion:** **2.Client:** **Name of Work:** **Order No. & Date:** **Cost:** **Date of completion:** **3. Client:** **Name of Work:** **Order No. & Date:** **Cost:** **Date of completion:** (**Necessary documents**)	**Copy of work completion certificates** (Enclosed / Not Enclosed) **Copy of work experience certificates** (Enclosed / Not Enclosed) **Note: Work Order/Purchase Order is not proof of work completion/experience certificate**
6	Whether experience from Private clients?	Experience of Non- Govt. Organization or private client, should submit copy of Bank Details / CA certificate and Bill Invoice in support of their claim for having experience of stipulated value of work (**Necessary documents**)	**Work experience Certificate** (Enclosed / Not enclosed) **TDS Certificate** (Enclosed / Not enclosed)
7	Turnover	Year INR (in Lacs)	
	Annualized average financial Turnover equivalent to Indian 30% of Estimated Cost/Amount during last three financial years.	**FY 2020- 21 (UDIN verified)** **FY 2021 - 22 (UDIN verified)** **FY 2022 - 23 (UDIN verified)** (**Necessary documents**)	**Proof of Turnover (Abridged Balance Sheet and Profit & Loss Account certified by Chartered Accountant, (UDIN verified)** (Enclosed / Not Enclosed)
	Average Rs.		
9	Undertaking for Registration Certificate in the format as given at Annexure-IV of tender/bid document	(**Necessary documents**)	Enclosed / Not Enclosed
10	Details of E-Performa in the format as given at Annexure-III of tender/bid document.	(**Necessary documents**)	Enclosed / Not Enclosed

11	Undertaking Regarding Blacklisting in the format given at Annexure-II of tender/bid document.	(**Necessary documents**)	Enclosed/Not Enclosed
12	Proforma for certificate of Net Worth from chartered accountant given at Annexure-V of tender/bid document.	**FY 2022 - 23 (UDIN verified)** (**Necessary documents**)	**Net worth Certificate for FY 2022-23** (Enclosed/Not Enclosed)
12	Details of any other information, if any		(Enclosed/Not Enclosed)

Signature
Authorized Signatory of the contractor/ Firm
(Signature with stamp)

(To be submitted along with Fee in Envelope – I)

Annexure-I

UNCONDITIONAL ACCEPTANCE LETTER

(To be uploaded in Fee/PQQ/Technical envelope)

(Tender/Bid ID: GEM/2024/B/4926424)

To,
The Director,
Indian Aviation Academy, Vasant Kunj, New Delhi
110070

Sub: Acceptance of Terms & Conditions of Tender/bid

Name of Work: **E-TENDER/BID FOR "Design, Development, Launching, Maintenance and associated services of e-Internship portal".**
Dear Sir,

The tender/bid document for the works mentioned above have been sold to me/us by Indian Aviation Academy and I / we hereby certify that I / we have read the entire terms and conditions of the tender/bid document made available to me / us in the office of The Director, Indian Aviation Academy, New Delhi, which shall form part of the contract agreement and I / we shall abide by the conditions / clauses contained therein.

1. I / We hereby unconditionally accept the tender/bid conditions of IAA's tender/bid document in its entirety for the above works.
2. It is clarified that after unconditionally accepting the tender/bid conditions in its entirety, it is not permissible to put any remarks / conditions (except unconditional rebates on quoted rates if any) in the tender/bid enclosed in envelope I and II and the same has been followed in the present case. In case any provisions of this tender/bid are found violated after opening the envelope I and II, I / we agree that the tender/bid shall be rejected and IAA shall without prejudice to any other right or remedy be at liberty to forfeit the full said earnest money absolutely.
3. That I/we declare that I/we have not paid and will not pay any bribe to any officers of IAA for awarding this contract at any stage during its execution or at the time of payment of bills and further if any officer of IAA ask for a bribe/gratification, I will immediately report it to the appropriate authority of IAA.

Yours Faithfully,

Date: _____ (Signature of the tender/bidder with rubber stamp)

Annexure-II

(To be submitted along with Pre-Qualifying cum Technical Bid in Envelope – I on his Letter Head)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

UNDERTAKING REGARDING BLACKLISTING

(Tender/Bid ID: GEM/2024/B/4926424)

I/we …….. (Name and post of authorized signatory) on behalf

……. (Name of firm) do here by solemnly affirm and declare as follow:

Our firm is not debarred / blacklisted by Indian Aviation Academy, Airports Authority of India or Central / State Govt Depts. / PSU Bank / ADB etc. and the debarment is not in force as on last date of submission of proposal. Our firm understand that in case above is discovered at later stage, our firm shall be liable for restrained from bidding in IAA, apart from any other appropriates contractual action including debarment/blacklisting, termination of the contract.

Date-:

[Signature and name of the authorized Signatory of the firm]

Place-:

Note: Above undertaking is to be given on a non-judicial stamp paper of Rs. 100/-

Annexure-III

(To be submitted along with Pre-Qualifying cum Technical Bid in Envelope – I on his Letter Head)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

Pro forma for e-Payment

(Tender/Bid ID: GEM/2024/B/4926424)

To
Director,
Indian Aviation Academy,
Vasant Kunj, New Delhi.

Subject: - Request for e-Payment.

Sir,

The following particulars are given below for effecting E-Payment in respect of our claim / bill.

1. Name of the Company :
2. Address :
3. Bank Account Number :
4. Bank Name :
5. Branch Address :
6. Branch Code :
7. IFSC Code of the Bank :
8. Permanent Account No. :

We are also enclosing herewith a cheque duly cancelled of our above Bank Account Number _____.

Thanking You

Yours faithfully,

Signature of Contractor
With rubber stamp

Annexure-IV

Undertaking of Registration Certificate
(Tender/Bid ID: GEM/2024/B/4926424)

(To be submitted along with Pre-Qualifying cum Technical Bid in Envelope – I on his Letter Head)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

I/We _____ (Name of company/ Firm) _____hereby undertakes that in case the Registration Certificate No. _____dated _____ issued by _____and Experience Certificate No._____ dated _____issued by _____(Name of Department)_____ submitted by me / us, is found to be forged /false at any stage, I / We may be debarred from IAA for taking participation in all future IAA works& any other suitable action may be taken against our company / firm as deemed fit by IAA.

Signature of Director / Proprietor of the Company / Firm With rubber-stamp.

****

ANNEXURE-V

CERTIFICATE OF NET WORTH FROM CHARTERED ACCOUNTANT

(To be submitted in Envelope-I)

(Tender/Bid ID: GEM/2024/B/4926424)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

"It is to certify that as per the audited balance sheet and profit & loss account during the financial year …….. the Net Worth of M/s ……. (Name & Registered Address of individual/firm/company), as on (the relevant date) is Rs. ……after considering all liabilities. It is further certified that the Net Worth of the company has not eroded by more than 30% in the last three years ending on (the relevant date)."

Signature of Chartered Accountant

…….

Name of Chartered Accountant

…….

Membership No. of ICAI

…….

Date and Seal

Annexure-VI

Proforma for Exit Management Plan

(Tender/Bid ID: GEM/2024/B/4926424)

(To be submitted along by successful bidder within 10 days after the award of the work)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

I/we ……. (Name and post of authorized signatory) on behalf …… (Name of firm) do here by solemnly affirm and declare as follow:

In any of the circumstances where:

(i) End of the contract period
(ii) Bankruptcy of the our company/firm
(iii) Violation of terms and conditions by us as specified in the tender document
(iv) IAA on it's discretion decides to remove the contractor by giving a notice period.
(v) Or any other case where the contract is getting closed or completed.

In any one of the above circumstances, M/s _____(Name of the Company) will follow the Exit Management Plan as described below:

a) Provide complete integrity of user data, course content and shall return back all the user information, course content to IAA.
b) All course related information has to be given back to IAA and no information in any aspect has to be withheld by the bidder before leaving the contract.
c) Shall clear all database, cache containing any information about IAA and cannot further host any of the IAA logo, name, image, course in any form on any platform whatsoever.
d) Duplicity/Copying or using of Course Content for any other purpose provided by IAA in any other form is strictly prohibited.
d) Violating of any of the above conditions shall be treated as breach of personal information and further actions shall be taken as deemed fit as per Information Technology Act.

Date-:

[Signature and name of the authorized Signatory of the firm]

Place-:

Note: Above undertaking is to be given on a non-judicial stamp paper of Rs. 100/-

Annexure-VII

PROFORMA BANK GUARANTEE FOR CONTRACT PERFORMANCE

(Tender/Bid ID: GEM/2024/B/4926424)

(To be stamped in accordance with Stamp Act)
(The non-judicial stamp paper should be in the name of issuing Bank)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal"

Ref : _____ Bank Guarantee No : _____
Date: _____

To
Director
INDIAN AVIATION ACADEMY
Vasant Kunj, New Delhi - 110070

Dear Sirs,

In consideration of the Indian Aviation Academy (hereinafter referred to as the Owner", which expression shall unless repugnant to the context or meaning thereof include its successors, administrators and assigns) having awarded to M/s --------- ---------- (hereinafter referred to as the 'Contractor', which expression shall unless repugnant to the context of meaning thereof, include its successors, administrators, executors and assigns), a contract. Bearing No. ---------- dated---------- valued at ---------- for ---------- and the contractor having (scope of contract) agreed to provide a Contract Performance of the entire Contract equivalent to ---------- -------(percentage as per GeM Bid Document) of the said value of the Contract to the Owner. We at ----------
(hereinafter referred to as the 'BANK', which expression shall, unless repugnant to the context or meaning thereof, include the successors, administrators, executors and assigns) do hereby guarantee and undertake to pay the Owner, on demand any and all money payable by the Contractor to the extent of ---------- as aforesaid at any time upto ---------- (day/month/year) without any demur, reservation, contest, recourse or protest and/or without any reference to the Contractor. Any such demand made by the owner the Bank shall be conclusive and binding notwithstanding any difference between the owner and contractor or any dispute pending before any court, tribunal or any authority.

The Bank undertakes not to revoke this guarantee during its currency without previous consent of the Owner and further agrees that the guarantee herein contained shall continue to be enforceable till the Owner discharges this guarantee. The Owner shall have the fullest liberty, without affecting in any way the liability of the Bank under this guarantee, to postpone from time to time the exercise of any powers vested in then or of any right which they might have against the Contractor. And to exercise the same at any time in any manner, and either to enforce or to forebear to enforce any convenants, contained or implied, in the Contract between the Owner and the Contractor or any other course of or remedy or security available to the Owner. The Bank shall not be released of its obligations under these presents by any exercise by the Owner or by any other matters or thing whatsoever which under law would, but for this provision, have the affect of relieving the Bank. The Bank also agrees that the Owner at its option shall be entitled to enforce this Guarantee against the
Bank as a principal debtor, in the first instance without proceeding against the Contractor and notwithstanding any security or other guarantee that the Owner may have in relation to the Contractors liabilities.

Notwithstanding anything mentioned herein above our liability under this guarantee is restricted to Rs. --------- and it shall remain in force upto and including ---------- and shall be extended from time to time for such period (not exceeding one year), as may be desired by M/s ---------- on whose behalf this guarantee has been given.
WITNESS

Dated this --------- day of ------- 2024 at -----

Signature ---------- Signature ----------

Name ---------- (Bank's Rubber Stamp)

Official address ---------- Name ----------

Designation with Bank Stamp
Attorney as per Power of

Attorney No. ----------

Date_____

Annexure-VIII

APPLICATION FOR EXTENSION OF TIME

(Tender/Bid ID: GEM/2024/B/4926424)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

Part-I

1. Name of the Contractor

2. Name of the work as given in the agreement

   (ii.) Agreement No. :-

   (iii.) Contract Amount :-

5. Date of Commencement of work as per agreement :-

6. Period allowed for completion of work as per agreement :-

7. Date of completion stipulated in agreement :-

8. Date of actual completion of work :-

9. Period for which extension is applied for. :-

10. Hindrances on account of which extension is applied for with dates on which hindrances occurred and the period for which these are likely to last.

Sl No	Name of Hindrance	Date of occurrence of hindrance	Date of over of hindrance	Period of hindrance	Overlapping Period	Net extension applied for	Remarks if any
1	2	3	4	5	6	7	8

Total period for which extension is now applied for on account of hindrances mentioned above.

Month Days

11. Extension of time required for extra work.

12. Details of extra work and the amount involved:-

Total value of extra work	Proportionate period of extension of time based on estimated amount put to tender on account of extra work.
(a)	(b)

13. Total extension of time required for 10 & 11.

Submitted to the Project Manager_____.

Signature of Contractor

Dated

Part II

(For Official Use)

1. Date of receipt of application from _____ Contractor for the work of _____ in the office of the Director, IAA _____.

2. Recommendations of the Project Manager as to whether the reasons given by the contractor are correct and what extension, if any, is recommended by him. If he does not recommend the extension, reasons for rejection should be given.

Dated: Signature of the Installation In-Charge

(To be filled in by the Project Manager)

1. Date of receipt in the office:-

2. Project Manager's remarks regarding hindrances mentioned by the contractor.

   (i) Serial No (if Any)
   (ii) Nature of hindrance
   (iii) Date of occurrence of hindrance
   (iv) Period for which hindrance is likely to last
   (v) Extension of time applied for by the contractor
   (vi) Overlapping period, if any, giving reference to items which overlap
   (vii) Net period for which extension is recommended
   (viii) Remarks as to why the hindrance occurred and justification for extension recommended.

3. Project Manager's Recommendations. The present progress of the work should be stated and whether the work is likely to be completed by the date up to which extension has been applied for. If extension of time is not recommended, what compensation is proposed to be levied under Clause 10 of General terms and Conditions.

Signature of Project Manager

Signature of Accepting Authority

****

Annexure -IX

Name of Work: "Design, Development, Launching, Maintenance and associated services of e-Internship portal"

Cyber Security guidelines

Cyber Security Protecting web resources from unauthorised use, access, changes, destruction, or disruption is generally termed as "Website Security" or "Secured Website".

- **Statement 1: Website, web application, web portal or mobile app must be Security Audited and an Audit Clearance certificate must be issued by NIC/ STQC/ STQC empanelled laboratory/CERT-In empanelled laboratory before hosting in production environment.**

  It should be ensured that the website, web application, web portal or mobile app don't have any security risks as identified by the latest OWASP Top 10 vulnerability list. The design and development agency or the developers should follow industry best practices such as OWASP ASVS and OWASP MAVS.

  Developer action: Securing critical web resources is more important than ever as the focus of attackers has steadily moved towards the application layer and they are exploiting the weaknesses in the code.

  A. Securing Code:

  (a) Ensure that all websites, web applications, web portals or mobile apps and their respective CMS, 3rd party plugins, codes, etc. are updated to the latest vers ions.
  (b) All passwords, connection strings, tokens, keys, etc. should be encrypted with salted hash. There should not be any plain passwords stored in config files or source code or in a database.
  (c) All exceptions should be handled appropriately. Custom error pages should be displayed for any errors/exceptions. At no point of time, a portion of source code should be displayed on the page in case of an error or exception.
  (d) HTTP Response Headers should be obscured.
  (e) Cookies should be secure and HTTP only.
  (f) Configure captcha for login pages.
  (g) Directory traversal should be disabled. In case of any specific attempt by a user to access a portion of the code by typing the URL path (ex: www.xxx.gov.in/js/custom.js) then the same should be redirected to a custom error page.
  (h) All default user names and IIS/Apache pages (like admin, default.aspx, index.aspx, etc.) should be renamed. The access URL for the admin panel/CMS, should also be renamed.
  (i) The Web Server processes should not be running under Administrator or Root user Account. A dedicated User account with limited privileges should be used for the Web Server Processes.
  (j) If the web or mobile app is integrated with any 3rd party Applications or using any APIs for external communication, then ensure that all such communications are done through encrypted channels.
  (k) Enforce strong password management policy, secure password recovery mechanisms and multi-factor authentication (MFA) for user login to website, web application or web portal infrastructure.
  (l) Implement role-based access control and minimal privilege policy for users as per need from the system.

(m) Establish the secure coding practices document based on leading practices such as OWASP for code development. Below is an indicative checklist that can be considered for secure code development:

(i) Input Validation
(ii) Authentication & Password Management
(iii) Session Management
(iv) Access Control
(v) Cryptographic Practices
(vi) Error Handling & Logging
(vii) Data Protection
(viii) Communication Security
(ix) System Configuration
(x) Database Security
(xi) File Management
(xii) Memory Management

(n) Implement logging functionality and periodically auditing the web logs for suspicious activity.
(o) Configure website, web application or web portal caching to optimize resource availability.
(p) Sanitise user input at both the client end and the server end with both syntactical as well as a semantic approach.
(q) The technology to be implemented should be chosen after careful consideration. Various client-side Active Content Technologies are available e.g., Java scripts etc. Each has its own strengths and weaknesses along with an associated risk.
(r) Disable the root user access to run the code on Linux/Unix hosts.
(s) Use explicit path names when invoking external programs and not rely on the PATH environment value.

B. Securing databases:

Database being the core of any application and/or organisation and is used to store large amounts of highly sensitive and personal information. Therefore, appropriate technical controls should be in place to safeguard the databases and information stored in them. The following are the guidelines for securing databases:

(a) Implement strong encryption and key management mechanism for the information both at rest and transit.
(b) Implement strong hashing and salting algorithms to store passwords in the database.
(c) Use secure credentials for database access. Remove or change all default database administrative passwords.
(d) Utilise strong passwords//phrases or implement multi-factor authentication.
(e) Disable unnecessary accounts such as orphaned accounts, unused accounts, generic and service accounts.
(f) Enable access to the database only from the Web Server on a whitelisted port and it should not be assigned publicly accessible IP.
(g) TLS should be enabled in databases for secure communications between web servers and databases.
(h) Create admin restrictions, such as by controlling privileged access on what users can do in a database.
(i) The application should use the lowest possible level of privilege when accessing the database.
(j) Turn on node checking to verify applications and users.
(k) Turn off all unnecessary database functionality (e.g., unnecessary stored procedures or services, utility packages, install only the minimum set of features and options required (surface area reduction)

(l) Enforce a strict access control policy and introduce role-based access control (RBAC) privileges.
(m) Enable audit trail logs on the database servers.
(n) Ensure appropriate logging and monitoring of database logs.
(o) Consider fine grained record/row level auditing based on the sensitivity of data.
(p) Implement a backup solution to store data and system configurations from the website, web application or web portal that should be backed up periodically.
(q) Keep the backup media file in safe custody and access to it should be restricted and logged.
(r) Conduct periodic auditing of Web Application - at least once in a year or as and when any changes are done in the source code, whichever is earlier.

Evaluator action: The evaluator shall check that the website/ web application/ web portal/ mobile app under evaluation has a valid security audit certificate issued by NIC/STQC/STQC empanelled laboratory/ CERT-In empanelled laboratory fulfilling CERT-In requirements.

- **Statement 2: Hosting Environment must be secured for ensuring confidentiality, integrity and availability (CIA).**

Think of a website's domain name as a street address. Now, think of the web host as the plot of "real estate" where the website exists online. As one would research a plot of land to build a house, it needs to examine potential web hosts to find the right one. Many hosts provide server security features that better protect a website and its data.

A. There are certain mandatory aspects to check for when choosing a hosting service provider (HSP):
(a) Ensure the hosting of the web infrastructure within geographical boundaries of India.
(b) The government organisation to ensure the HSP is providing data centre, business continuity plan and disaster recovery environments with state-of-the-art secure infrastructure configured in high availability (HA) mode for hosting the websites, web applications, web portals or mobile apps and their respective CMS.
(c) Conduct periodic drills of disaster recovery environment - at least once in a year.
(d) HSP to ensure that the servers are protected against environmental, physical and cyber threats.
(e) Ensure the HSP has implemented all security controls of the Data Centre including physical security and appropriate access control mechanisms.
(f) Servers, Network devices used to host the website should be hardened with latest security patches and periodic Vulnerability Assessment (VA) and Penetration Testing (PT) followed by corrective actions should be performed as per the security policy.
(g) Ensure the HSP of the hosting environment has deployed and configured a Web Application Firewall (WAF), which is hardened with latest security patches and is available for use by the government organisation on demand.
(h) Enable and maintain logs of the ICT infrastructure for a rolling period of 180 days as per CERT-In directions.
(i) Regularly monitor and conduct review of alerts and logs
(j) HSP should also ensure:
    (i) Web host offer a Secure File Transfer Protocol (SFTP);
    (ii) FTP use by unknown users is disabled; and
    (iii) It uses a rootkit scanner.
(k) HSP should ensure to secure the containerized environments, if applicable.

B. Best practices should be used to protect the containerized environments:
(a) Each library and tool pulled into the image poses a potential threat. To mitigate these threats, one need to include the application within the container image. This should be statically compiled binary that contains all required dependencies.

(b) Remove all components the application does not need. For example, remove the "sed" and "awk" binaries, which are present by default on any UNIX system. This can help reduce the attack surface.
(c) If the image is not created from scratch, only trustworthy images should be taken. Public image repositories, such as Docker Hub, can be used by anyone and may contain malware or misconfigurations.
(d) If there is a private registry, the system administrator has to establish access controls that define exactly who can access and publish images and who cannot perform such actions.
(e) Signatures help track images to the people who signed them. This makes it difficult to substitute the signed image for a compromised one. The Docker Content Trust mechanism provides information about signing images. Notary - an open-source tool can help sign and verify images.
(f) Vulnerability scanners are designed to identify known vulnerabilities. These tools can help find critical vulnerabilities and detect critical threats. Scanners can be used on a continuous basis to ensure that the registries do not contain critical vulnerabilities.
(g) Secure the target environment – by hardening the underlying host operating system. It can also be established that the firewall and VPC rules or create special accounts that limit access.
(h) Use an orchestration platform – These systems usually provide secure API endpoints as well as role-based access control (RBAC), which can help minimise the risk of unauthorised access.
(i) Use immutable deployments – This involves creating an instance image during the build steps. The deployment can then use this image to create new instances. To update the application, new images should be created, spin up new instances and then destroy the old ones.
(j) Create separate virtual networks for the containers – This introduces a level of isolation that can reduce the attack surface.
(k) Apply the principle of least privilege – Allow connectivity only between containers that truly need it.
(l) Expose only the ports that serve the application – Do not expose any other ports, except for SSH. Apply this principle to containers as well as the underlying machines.
(m) Use TLS to secure communication between services – This process encrypts traffic and ensures only authorised endpoints are allowed.
(n) Use the Docker Image policy plugin – This plugin is designed to prevent any process from pulling images that were not previously allow-listed.
(o) Enable TLS everywhere – enable TLS for all supported components to defend against traffic sniffing and authenticate identities at both ends of each connection.
(p) Use a service mesh architecture – Service meshes are networks of persistent encrypted connections between high-performance sidecar proxies. They provide traffic monitoring, management and policy enforcement without affecting microservices.
(q) Use OPA – Open Policy Agent (OPA) enforces custom policies on a Kubernetes object without reconfiguring or recompiling the Kubernetes API server.
(r) Apply network policies – The default Kubernetes networking permits all traffic between pods, but can be restricted with a network policy.
(s) Implement private networks – Deploy each Kubernetes worker and master node on a private subnet to secure the connections to corporate networks, make nodes unreachable from the public Internet and minimise overall attack surface.
(t) Keep the etcd cluster separate – Use a firewall to protect the etcd cluster, which stores state and secret information and requires special protection compared to other Kubernetes components.
(u) Ensure the regular rotation of encryption keys – Regularly rotating encryption keys and certificates helps minimise the blast radius of an attack that compromises keys.
(v) Use static analysis for YAML – Statically analyse where pod security policies deny access to API servers. This should be part of the development workflow because it helps identify the organisation's risk tolerance and conformity requirements.
(w) Manage secrets – Integrate clusters using a secret management system to ensure application pods automatically receive all secrets and passwords needed at runtime (based on the app roles associated with each pod).

(x) Check the code – Scan the code and use static analysis to ensure automation security. Source code must be scanned for all application code in Kubernetes to identify vulnerabilities and hard-coded errors.

(y) Use RBAC policies based on the principle of least privilege – Role-based access control (RBAC) helps manage access policies at a granular level to protect resources. A centralised authentication and authorization system like single sign-on throughout the organisation makes onboarding and offboarding easier.

Developer action: Following activities are to be ensured by the developer, which in this case would mean its system administrator, or/and DevOps:
(a) Restrict the admin access and implement the principle of least privilege and disable unnecessary accounts and privileges;
(b) Disable all unnecessary ports opened on the web server, i.e., deny all access by default;
(c) Remove default, temporary or guest accounts from the web server; and
(d) Change the default login credentials and implement strong password enforcement with password expiration policy on the web server.
(e) Whitelist the application in use and disable the unused features or modules.
(f) Use of Secure FTP (SFTP) to transfer files over an encrypted channel.
(g) Disable Hypertext Transfer Protocol (HTTP) and enforce Hypertext Transfer Protocol Secure (HTTPS) & HTTP Strict Transport Security (HSTS). To keep a website safe, it needs a secure URL. If a user uses their private information to access a site, it should use HTTPS, not HTTP, to deliver it.
(h) Mandatorily use a valid SSL Certificate on all websites. The SSL Certificate should use at least 2048-bit SHA 256 encryption or higher.
(i) Ensure that the SSL Certificate is valid and keep track of the certificate expiry date and take necessary action to renew/replace the certificate before expiry.
(j) Configure the HTTP Service banner so that Web Server and Operating System type & version will not be disclosed.
(k) The configuration files of the Web Server must be protected by the Web Server process. One can find them in the root web directory. Web server configuration files permit to administer server rules. This includes directives to improve website security. There are different file types used with every server, following may be referred for their usage:
    (i) Apache web servers use the .htaccess;
    (ii) Nginx servers use nginx.conf; and
    (iii) Microsoft IIS servers use web.config.
(l) Open source/Freeware software should be used with due diligence.
(m) Remove or disable all superfluous drivers, services and software.
(n) Remove or replace obsolete software libraries.
(o) Remove or replace outdated security level protocols.
(p) Limit unauthorised or unauthenticated or administrative privileged user access to the system.
(q) Implement encryption for the transmission of all sensitive information. This should include TLS for protecting the connection. Disable weak cyphers (SSLv2, SSlv3, 3DES, RC4, TLS v1.0, v1.1).
(r) Periodically review logs for suspicious activity like authentication, user access activity & changes and privilege elevation & usage.
(s) Implementation of network segmentation and segregation to limit the impact of network intrusion.
(t) There should be no active concurrent sessions of the web server.
(u) Ensure servers, frameworks and system components are running the latest approved version and have all patches issued for the version in use.
(v) Isolate development environments from the production network and provide access only to authorised development and test groups.

(w) Implement a software change control system to manage and record changes to the code both in development and production.
(x) Establish practice of hardening web servers and conduct the periodic secure configuration review of the same.

(y) The most common attacks against websites are entirely automated. What many attack bots rely on is for users to have their CMS settings on default. After choosing a CMS, change default settings immediately. Changes help prevent a large number of attacks from occurring. CMS settings can include adjusting control comments, user visibility and permissions e.g., default setting change using 'file permissions.' Permissions can be changed to specify who can do what to a file. Each file has three permissions and a number that represents every permission:

(i) 'Read' (4): View the file contents.
(ii) 'Write' (2): Change the file contents.
(iii) 'Execute' (1): Run the program file or script.
(iv) To clarify, to allow multiple permissions, add the numbers together e.g., to allow read (4) and write (2), set the user permission to (6.) Along with the default file permission settings, there are three user types:
(I) Owner – Often, the creator of the file, but ownership can be changed. Only one user can be the owner at a time.
(II) Group – Each file is assigned to a group. Users who are part of that specific group will gain access to the permissions of the group.
(III) Public – Everyone else.

(z) Customise users and their permission settings. Do not keep the default settings as is, otherwise it shall run into website security issues at some point.
Evaluator action: The evaluator shall check to ensure that the Government organisation actions are being complied.

- **Statement 3: Website must have the Security Policy, Privacy Policy and the Contingency Management Plan clearly defined policies and plans approved by the government organisation.**

It should be clearly defined and approve the website/app related policies listed above. Web Information Manager must ensure their implementation throughout the website/app life cycle.

Developer action: Citizen-facing policies like copyright policy, privacy policy and terms and conditions must be published on the website.

Evaluator action: The evaluator will:
(a) Compare during the backend audit the policies given in WQM and those available at the website/app for consistency.
(b) Check the implementation of these policies by examining the documented records generated by the implementation.

Guidelines for Cyber Security Audit

1. Comprehensive audit:
1.1 Comprehensive audit should be done at least once in a year and should cover the entire application, including the following:
(a) web application (both thick client and thin client);
(b) mobile apps;
(c) APIs (including API whitelisting);
(d) databases;

(e) hosting infrastructure and obsolescence;
(f) cloud hosting platform and network infrastructure; and
(g) Aadhaar security compliance as mandated under the Aadhaar Act, 2016, the regulations made thereunder and Aadhaar Authentication Application Security Standard available on UIDAI's website (irrespective of whether or not the application owner/administrator is a requesting entity under the Act, the cybersecurity compliance for Aadhaar use should be benchmarked against the said standards as the relevant information security best practice, including, in particular, use of Aadhaar Data Vault for storage of Aadhaar number and Hardware Security Module for management of encryption keys).

1.2 The scope of the comprehensive audit should include, *inter alia,* the following:
(a) source code assessment;
(b) application security assessment (both Black Box and Grey Box testing), including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis.
(c) network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs).
(d) penetration testing.
(e) network and device configuration review.
(f) application hosting configuration review.
(g) database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication).
(h) user access controls (including privilege access management) and access reconciliation review.
(i) identity and access management controls review.
(j) data protection controls review (*inter alia*, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]")
(k) security operations and monitoring review (including maintenance of security logs, correlation and analysis)
(l) review of logs, backup and archival data for access to personal data (including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law) and
(m) review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website).
1.3 The auditor should be CERT-In-empanelled and, in case of application hosted on cloud, the auditor and should have the capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website.

2. Limited audit

2.1 Limited audit shall be performed six months after the comprehensive audit, and should be carried out even earlier if there is:

(a) modification in application functionality or
(b) addition/modification of APIs or
(c) migration to new infrastructure platform or cloud service or
(d) change in configuration of application hosting, servers, network components and security devices or
(e) change in access control policy.

2.2 The scope of limited audit should include, *inter alia*, the following:

(a) *In all cases:* Source code assessment; application security assessment (both Black Box and Grey Box testing) including as per OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis.

(b) *In case limited audit is after six months of comprehensive audit:* In addition to (a) above, user access controls (including privilege access management) and access reconciliation review; identity and access management controls review.

(c) *In case limited audit is done earlier:* In addition to (a) and (b) above,

(i) *For audit on modification in application functionality, addition/modification of APIs, migration to new infrastructure platform or cloud service or change in configuration of application hosting, servers, network components and security devices:* Network vulnerability assessment (including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs); network and device configuration review; application hosting configuration review; database security assessment (including whether personal data is being encrypted at rest and in motion, or used in tokenised form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorised users and are protected with multifactor authentication); data protection controls review (*inter alia*, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]"); security operations and monitoring review (including maintenance of security logs, review of logs, integration with security monitoring solutions, correlation and analysis; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law) review of logs, backup and archival data specifically for access to personal data; review of key management practices (including secure storage and exchange of encryption keys, configuration and use of Aadhaar Data Vault as detailed in the Aadhaar Authentication Application Security Standard available on UIDAI's website); and

(ii) *For audit on change in access control policy:* Review of logs and integration with security monitoring solutions.

2.3 Auditor should be a CERT-In-empanelled auditor who is other than the auditor who has done the last comprehensive audit. Further, in case the application is hosted on cloud, the auditor should have capability for carrying out cloud security audit as per the empanelment details available on CERT-In's website.

2.4 Alternatively, in case there is an information security audit vertical of the organisation hosting and/or managing the application which—

(a) satisfies the baseline requirements specified for CERT-In empanelment in CERT-In's Guidelines for applying to CERT-In for Empanelment of IT Security Auditing Organisations and

(b) is independent of the ICT vertical with the head of such vertical having direct reporting line to the head of the organisation, such information security audit vertical may perform internal audit.

3. Role of the application owner

3.1 The application owner (Ministry/Department/organisation concerned, as applicable) should—

(a) appoint the auditor and initiate the audit process as required;

(b) extend necessary support and access for the audit;

(c) meet the cost of audit; and

(d) ensure requisite follow-up for closure of audit findings, including in terms of securing requisite approvals and resources and coordinating among the application developer, application manager, hosting service provider, Web Information Manager / Chief Information Officer and CISO.

Type of Vulnerabilities

Different type of vulnerabilities may occur at Web portal, Website & Applications as cyber threats which need to be addressed if any before production of Web portal, Website & Applications & mitigate on every update.

Some of the vulnerabilities are listed below:

S.N.	Application	Type of vulnerability
1	Web Portal	Directory Listing
2	Web Portal	Back & Refresh Attack
3	Web Portal	Clear text submission of Credentials
4	Web Portal	Missing X-Frame-Options header
5	Web Portal	Weak Ciphers
6	Web Portal	Server Version & Technology Version disclosure
7	Web Portal	OPTIONS Method Enabled
8	Web Portal	Misconfirgured Access Control Allow Origin header
9	Web Portal	CSP Response Header is Missing
10	Web Portal	HTTP Strict Transport Security is not set
11	Web Portal	X Content Type Options Header Missing
12	Website	Clear text submission of Credentials
13	Website	Concurrent Login
14	Website	Dangerous HTTP method allowed
15	Website	Improper Input Validation
16	Website	Using Component with known Vulnerablities
17	Website	Cookie Secure, samesite attribute is not set
18	Website	OPTIONS Method enabled
19	App(Android)	JS Enabled in webview
20	App(Android)	Weak hashing algorithm used
21	App(Android)	Tap Jacking

22	App(Android)	No Checks implement for Screen Mirror Application
23	App(Android)	Improper Input Validation
24	App(iOS)	No Checks implement for Screen Mirror Application
25	App(iOS)	Insecure App Transport Security (ATS) Settings
26	App(iOS)	Snapshot enabled
27	App(iOS)	Concurrent Login

****

Annexure-X

Name of Work: Design, Development, Launching, Maintenance and associated services of e-Internship portal

Checklist for Comprehensive Security Audit (CSA)

Vulnerability Assessment and Penetration Testing (VAPT) Checklist Document(For audit of important government applications/databases)

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
1	ISOG	**Information Security Organisation and Governance** **Check for information security organisation structure, governance framework and information security policies applicable for the audit entity / organisation.** **For any outsourced function or managed services operations by external agency, check for the third party / vendor governance, management and information security compliances.**			

2	**ISOG.1**	**Information Security Organisation**	**To determine whether the audit entity / organisation have a CISO function that oversees information security governance and compliances.**		
3	ISOG.1.1	1. Check whether the auditee organisation has appointed a dedicated CISO / Information Security Officers to oversee and enforce information security practices within the organisation.			
4	ISOG.1.2	2. Where applicable, check whether auditee organization has an independent Data Privacy Officer (DPO) to oversee and enforce data protection and privacy compliance requirements in accordance with country's data protection act and/or sectoral regulatory mandates.			
5	**ISOG.2**	**Information Security Organisation**	**To determine whether the CISO function have independent reporting to entity's Board of Directors / CEO.**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
6	ISOG.2.1	1. Check for the documented and approved information security organisation structure. Wherever applicable, also check for the information privacy organization structure and processes.			
7	**ISOG.3**	**Information Security Governance**	**To determine whether the audit entity / organisation follow established information security practices in reference to ISO27001 (ISMS), NIST Cyber Security Framework, CSA Framework, ISO27701 (PIMS) and other industry leading standards.**		
8	ISOG.3.1	1. Check for the information security and privacy certification of the audit entity / auditee organisation. Check valid ISO27001 certification at deployment location			
9	ISOG.3.2	Incorporation/Adherence to Meity and Cert-In guidelines			
10	**ISOG.4**	**Information Security Governance**	**To determine whether the audit entity / organisation performs periodic (annual / half yearly / quarterly, as applicable) review of information security risks and compliances of its ICT applications and infrastructure in accordance with the leading industry standards as mentioned in ISOG.3** **To determine whether there is an established third party information security policy and whether the third party information security risks and compliances were**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			documented and reviewed by auditee organization's CISO / Security Officer / Board. **(Where applicable, for external suppliers / vendors / outsourced managed services operations that manage or maintain the ICT applications and/or infrastructure)**		
11	ISOG.4.1	1. Check for adequacy of governance review process and periodicity of reviews.			
12	ISOG.4.2	3. Review the action taken by management of audit entity to address the risks and non-compliances / open observations / open vulnerabilities. Check last Application Security Audit, VAPT status as per the adopted Security Audit Policy. Check for the past audit reports and vulnerabilities reported by internal auditors and/or CERT-In auditors. Check for past 1 year audit reports. Review the frequency and completeness of network vulnerability assessments, DC/DR, existence of network segmentation to isolate critical assets and enhance overall network security. Determine the implementation of encryption protocols to secure sensitive data transmitted over the network.			

13	ISOG.4.3	1. Understand the 3rd party / vendor / supplier ecosystem of the audit organizations and identify the critical ICT infrastructure (e.g. application development and upgrade,			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		Data Center support / operations, security infrastructure configurations and administration etc.)			
14	ISOG.4.4	2. Check for the 3rd party information security policy. Check for 3rd party information security risks and compliances documentation / reports for open / critical risks and issues.			
15	ISOG.4.5	Check processes and procedures for monitoring adherence to established information security requirements for each type of supplier and level of access, including third-party reviews and product validation/certification by recognized authority. Check for standardized process and lifecycle for managing supplier relationships (such as NDA signing) with each of the supplier			
16	**A**	**Source Code Assessment (SAST)**	**Source code assessment should be performed for all in-scope applications (including web applications and mobile applications) and API's**		
17	**A.1**	**Planning and Information Gathering**	**To determine whether application deployment and security architecture is documented and depicts at minimum the following:** **- Servers** **- Applications (incl. web & mobile apps)** **- API's** **- IP schema details** **- interfaces with database(s)** **- PII data flow**		
18	A.1.1	1. Identify the application testing scope and plan the testing methodology.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
19	A.1.2	2. Guidance for certain minimum checks include the following:			
20	A.1.2.1	a) Deployment architecture documented plan depicting (Servers, applications, APIs, IP Schema details and interfaces that access the database) should be made available.			
21	A.1.2.2	b) Inspect the page source for sensitive PII info. Manually explore the site and Review the web Contents			
22	A.1.2.3	c) Check whether only web Interface or both Mobile and Web Interface is available			
23	A.1.2.4	d) Check for last Audit compliance status			
24	A.1.2.5	e) Spider/crawl for missed or hidden content. Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store			
25	A.1.2.6	f) Check the caches of major search engines for publicly accessible sites			
26	A.1.2.7	g) Check for differences in content based on User Agent (e.g. mobile sites, access as a search engine crawler)			
27	A.1.2.8	h) Perform Web Application Fingerprinting			
28	A.1.2.9	i) Identify technologies used and Identify user roles			
29	A.1.2.10	j) Identify application entry points and Identify client-side code			
30	A.1.2.11	k) Identify multiple versions/channels (e.g. web, mobile web, mobile app, web services)			
31	A.1.2.12	l) Identify co-hosted and related applications			
32	A.1.2.13	m) Identify all hostnames and ports			
33	A.1.2.14	n) Identify third-party hosted content			
34	A.1.2.15	o) Perform Reconnaissance via Google Dorks Search			
35	A.1.2.16	p) Script output of web folder for assessment of clean data			
36	A.1.2.17	q) Check and examine the permission of read & write folder			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
37	**A.2**	**Secure Application Development / Coding practices**	**To determine whether secure application development practice / process exists in the auditee organisation.**		
38	A.2.1	1. Inquire with application owner and application developer to understand the application development methodology.			
39	A.2.2	2. Check for DevSecOps (CI/CD pipeline based Security operations) processes and/or security checkpoints/tollgate process for application development. Check whether Code review (Source Code Analysis) Process is part of the development process or not.			
40	A.2.3	3. Validate code adherence to established coding standards, industry guidelines and assessment frequency during SAST assessments and check whether developers are trained on secure coding practices.			
41	A.2.4	4. Check whether there is separate development / staging environment and production environment.			
42	**A.3**	**Version Management and Release Management**	**Review the application code version and the major/minor changes committed in the version management tool (e.g. SVN, BitBucket, Gitlab etc.).**		
43	A.3.1	1. Check for major and minor code releases committed in the version management tool and the change description.			
44	A.3.2	2. Check for the release management process and approvals workflow. Check if approvals are provided by Change Advisory Board (CAB) or authorized personnel from senior management in change of application security. Check for approval records. Check if source code handling is limited to authorized users only.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
45	**A.4**	**Automated Source Code Scanning & Manual Code Analysis**	**Perform automated source code scan using a reliable open-source or proprietary scanning tool such as Fortify, SonarQube, Checkmarx etc. and assess for vulnerabilities (in accordance with OWASP Testing Guide and CERT-In's Guidelines for Secure Application, Design, Implementation and Analysis).** **Perform manual code review to identify the following vulnerabilities in the source code- sensitive information disclosure (including hard-coding of PII data, PII tokens, authentication tokens, security keys, encryption keys, passwords / user credentials, etc.)**		
46	A.4.1	1. Utilize the SAST tool to identify and prioritize high risk vulnerabilities (refer OWASP testing guide and CERT-In guidelines).			
47	A.4.2	2. Verify that the SAST tools are configured to check for compliance with coding standards and security policies.			
48	A.4.3	3. Review the results of automated scans to ensure comprehensive coverage of the codebase.			
49	**B**	**Application Security Assessment (both Black Box and Grey Box)**	**Assessment should be performed as per OWASP Testing Guide and CERT-In Guidelines for Secure Application Design, Implementation and**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			Analysis		
50	**B.1**	**Application Security Testing**	**Perform application security testing using reliable open-source or proprietary application security tools such as OWASP ZAP, Acunetix, Burp Suite etc. and assess for vulnerabilities (in accordance with OWASPTesting Guide and CERT-In guidelines for secure application design, implementation and analysis).**		
51	B.1.1	1. Check for application authentication, authorization session management, etc.			
52	B.1.2	2. Examine error messages for application sensitive information disclosure or internal server leakage details			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
53	**B.2**	**Application and API Hosting Security Configurations, Data Transmission and Encryption and Application Functionality Security Assessment**	**Review the application security configurations including secure data transmission (TLS, SSL) and encryption configurations to protect sensitive information / data to determine that latest / secure encryption protocols have been deployed.** **Review the application access and authentication configurations / parameters and test whether user authentications can be bypassed or leveraged for admin/privileged users.** **Review the application features, functionality and test for potential misuse of application business logic and denial of service.** **Review the application/ API whitelisting and secure API linkages to determine whether access to applications and API's is limited to authorized users and systems only.**		
54	B.2.1	1. Check for the following authentication configurations:			
55	B.2.1.1	a) Check for user enumeration			
56	B.2.1.2	b) Check for authentication bypass			
57	B.2.1.3	c) Check for brute force protection			

58	B.2.1.4	d) Check password security controls such as quality rules, autocomplete on password forms/input, change process, reset			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		and/or recovery, password is salted hashed (e.g. SHA256, SHA512)			
59	B.2.1.5	e) Check remember me functionality			
60	B.2.1.6	i) Check integrity and security of CAPTCHA			
61	B.2.1.7	j) Check multi factor authentication			
62	B.2.1.8	k) Check for logout functionality presence			
63	B.2.1.9	l) Check for cache management on HTTP (e.g. Pragma, Expires, Max-age)			
64	B.2.1.10	m) Check for default logins			
65	B.2.1.11	n) Check for user-accessible authentication history			
66	B.2.1.12	o) Check for out of channel notification of account lockouts and successful password changes			
67	B.2.1.13	p) Check for consistent authentication across applications with shared authentication schema / SSO			
68	B.2.1.14	r) Check whether Salt is generated at client side or server side			
69	B.2.1.15	s) Check for clipboard data stealing attack			
70	B.2.2	2. Check for the following Session Management configurations:			
71	B.2.2.1	a) Establish how session management is handled in the application (e.g. tokens in cookies, token in URL)			
72	B.2.2.2	b) Check session tokens for cookie flags (HTTP Only and secure)			
73	B.2.2.3	c) Check session cookie scope (path and domain)			
74	B.2.2.4	d) Check session cookie duration (expires and max-age)			
75	B.2.2.5	e) Check session termination after a maximum lifetime			
76	B.2.2.6	f) Check session termination after relative timeout			
77	B.2.2.7	g) Check session termination after logout			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
78	B.2.2.8	h) Check to see if users can have multiple simultaneous sessions			
79	B.2.2.9	i) Check session cookies for randomness			
80	B.2.2.10	j) Confirm that new session tokens are issued on login, role change and logout			
81	B.2.2.11	k) Check for consistent session management across applications with shared session management			
82	B.2.2.12	l) Check for session puzzling			
83	B.2.2.13	m) Check for CSRF and clickjacking			
84	B.2.3	3. Check for the following data validation configurations:			
85	B.2.3.1	a) Check for Reflected, Stored, DOM based Cross Site Scripting and Cross Site Flashing			
86	B.2.3.2	b) Check for Injections related vulnerabilities such as HTML injection, SQL Injection, LDAP injection, ORM Injection, XML, XXE, SSI Injection, IMAP/SMTP injection, code, command injection, host header injection etc.			
87	B.2.3.3	c) Check for Front end web interface (as per OWASP top 10)			
88	B.2.3.4	d) Check for Overflow (Stack, Heap and Integer)			
89	B.2.3.5	e) Check for Format String			
90	B.2.3.6	f) Check for incubated vulnerabilities			
91	B.2.3.7	g) Check for HTTP Splitting/Smuggling			
92	B.2.3.8	h) Check for HTTP Verb Tampering			
93	B.2.3.9	i) Check for Open Redirection			
94	B.2.3.10	j) Check for Local File, Remote File Inclusion			
95	B.2.3.11	k) Compare client-side and server-side validation rules			
96	B.2.3.12	l) Check for NoSQL injection			
97	B.2.3.13	m) Check for HTTP parameter pollution			

98	B.2.3.14	n) Check for auto-binding			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
99	B.2.3.15	o) Check for Mass Assignment			
100	B.2.3.16	p) Check for NULL/Invalid Session Cookie			
101	B.2.3.17	q) Check for Server-side request forgery			
102	B.2.3.18	r) Check for maximum character limit in Input box / Field			
103	B.2.4	4. Check for authorization vulnerabilities			
104	B.2.4.1	a) Check for path traversal			
105	B.2.4.2	b) Check for bypassing authorization schema			
106	B.2.4.3	c) Check for vertical Access control problems (a.k.a. Privilege Escalation)			
107	B.2.4.4	d) Check for horizontal Access control problems (between two users at the same privilege level)			
108	B.2.4.5	e) Check for missing authorization			
109	B.2.5	5. Check for application configurations to prevent denial of service attacks			
110	B.2.5.1	a) Check for anti-automation			
111	B.2.5.2	b) Check for account lockout			
112	B.2.5.3	c) Check for HTTP protocol DoS			
113	B.2.5.4	d) Check for SQL wildcard DoS			
114	B.2.5.5	e) Check for OTP Flooding			
115	B.2.5.6	f) Check for Captcha used cannot be replayed after getting validated			
116	B.2.6	6. Check for business logic misuse			
117	B.2.6.1	a) Check for feature misuse			
118	B.2.6.2	b) Check for lack of non-repudiation			
119	B.2.6.3	c) Check for trust relationships			
120	B.2.6.4	d) Check for integrity of data			
121	B.2.6.5	e) Check segregation of duties			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
122	B.2.6.6	f) Check for business logic flaw for complete application workflow			
123	B.2.6.7	g) Check for proper input validation			
124	B.2.6.8	h) Check for concurrent user login misuse			
125	B.2.6.9	i) Check for application session timeout			
126	B.2.6.10	j) Check that acceptable file types are whitelisted			
127	B.2.6.11	k) Check that file size limits, upload frequency and total file counts are defined and are enforced			
128	B.2.6.12	l) Check that file contents match the defined file type			
129	B.2.6.13	m) Check that all file uploads have Anti-Virus scanning in-place.			
130	B.2.6.14	n) Check that unsafe filenames are sanitized			
131	B.2.6.15	o) Check that uploaded files are not directly accessible within the web root			
132	B.2.6.16	p) Check that uploaded files are not served on the same hostname/port			
133	B.2.6.16	q) Check that files and other media are integrated with the authentication and authorization schemas			
134	B.2.6.17	r) Open file upload may be avoided			
135	B.2.7	7. Check for Application API whitelisting			
136	B.2.7.1	a) Check for API Security (as per OWASP top 10 and any directions related to application security as issued by UIDAI)			
137	B.2.7.2	b) Check how external APIs consumed are handled properly			
138	B.2.7.3	c) Check how APIs released are handled			
139	B.2.7.4	d) For thick client based applications, check if application is running on an untrusted system, ensure that thick client should always connect to the backend through an API that can enforce appropriate access control and restrictions. Also,			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		check that Direct connections should never be made from a thick client to the backend database.			
140	B.2.7.5	e) For mobile apps, check for mobile app secure API linkages			
141	B.2.7.6	f) For HTML5 based apps, check for web messaging, web storage SQL injection, CORS implementation (refer CERT-In guidance) and offline web application misuse.			
142	B.3	Assess whether the application is transmitting the information in an encrypted format based on leading encryption standard such as TLS 1.3. Check that deprecated / obsolete encryption protocols / TLS protocols are not configured.			
143	B.4	Check if there are potential man-in-the-middle attack related vulnerabilities in application data transmission.			
144	B.5	Check for the following cryptography and secure transmission configurations:			
145	B.5.1	1. Check for randomness functions			
146	B.5.2	2. Check SSL/TLS Version, Algorithms, Key length, weak ciphers			
147	B.5.3	3. Check for Digital Certificate Validity (Duration, Signature and CN)			
148	B.5.4	4. Check credentials only delivered over HTTPS			
149	B.5.5	5. Check that the login form is delivered over HTTPS			
150	B.5.6	6. Check session tokens only delivered over HTTPS			
151	B.5.7	7. Check if HTTP Strict Transport Security (HSTS) in use			
152	B.5.8	8. Check how Sensitive/PII Data at rest is stored			
153	B.5.9	9. Check how Sensitive/PII Data in transit (like Aadhaar Card, PAN, Credit/Debit Card Number, Password etc.) is			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		handled and stored (check that deprecated encryption protocols is not used)			
154	B.5.10	10. Check how Sensitive/PII Data in use (i.e. Back-end data) is handled			
155	B.6	Security of Sensitive Data			
156	B.6.1	1. Check if sensitive data at rest and in transit encryption is done properly			
157	B.6.2	2. Check for wrong algorithms usage depending on context			
158	B.6.3	3. Check for weak algorithms usage			
159	B.6.4	4. Check for proper use of salting			
160	**C**	**Network Vulnerability Assessment**	**(including regarding whether an inventory exists of computers, network and software components and URLs, along with details of authorized asset user and IP, AMC, patch management, antivirus, software license, asset version and corresponding end of life/support particulars; whether centralized platform exists for pushing patch updates and antivirus and there is centralized visibility of assets; and whether periodic review has been undertaken to remove/replace obsolete assets and remove unused URLs)**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
161	**C.1**	**Network Security Architecture Review**	**Review the network security architecture design and determine the following: - Whether application, databases and underlying infrastructure is protected for external network attacks (i.e. through use of Zero Trust Network Architecture, Firewalls, IPS/IDS, Anti-DDoS)** **- Whether the network segmentation and network zoning is implemented to protect the application hosting environment.** **- Whether critical databases hosting sensitive / PII data is not exposed over internet.**		
162	C.1.1	1. Verify that authorization, security controls and access controls are in place, protecting and restricting network access to authorized personnel only.			
163	**C.2**	**Network Security Patches**	**Review network asset inventory to determine whether inventory is updated and reviewed periodically.** **Review the patch management process to determine that critical security patches are implemented on vulnerable network equipment.** **Review the Network devices for their end of life and security operations support.**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
164	C.2.1	1. Check the existence of an up-to-date inventory detailing computers, network components, software, and authorized asset details including users, IPs, AMCs, patch management, antivirus, and software licenses.			
165	C.2.2	2. Confirm the presence of a centralized platform for patch updates / deployment, ensuring centralized visibility of all assets.			
166	C.2.3	3. Inquire whether asset versions and corresponding end-of-life/support details are documented, up-to-date in the inventory and periodically reviewed.			
167	C.2.4	4. Check that security patches and updates are implemented periodically (as per their release) and tested before deployment.			
168	C.2.5	5. Check that latest security patches have been installed.			
169	C.2.6	6. Check that there are no end-of-life / obsolete network devices that are vulnerable to security threats.			
170	**C.3**	**Network Monitoring**	**Review the Network operations and monitoring process to determine whether the network traffic is monitored for unauthorized access and usage.**		
171	C.3.1	1. Check the adequacy of network monitoring tools and technologies to detect and respond to potential network security incidents.			
172	C.3.2	2. Check the network performance and network security incident logs.			
173	**C.4**	**Auditing Business Continuity and Disaster Recovery (BCP/DR)**			

174	C.4.1	1. Has the organization performed a comprehensive asset inventory and assigned business owners to all assets?			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
175	C.4.2	2. Has the Project specific Business Impact Analysis (BIA) performed as a part of their BCP/DR plans?			
176	C.4.3	3. Have all the organization's personnel been trained in their role in the BCP/DR process? . Are all BCP/DR plans tested and kept up-to-date on a regular basis?			
177	C.4.5	5. Is the organization regularly backing up their information systems onsite and offsite in light of their BCP/DR plans?			
178	**D**	**Penetration Testing**			
179	**D.1**	**Penetration Testing Scope and Coverage**	**Review the network penetration testing policy to determine the periodicity and coverage of network penetration tests.** **Review the past penetration testing reports to determine whether penetration tests covered the critical assets and network segments. Review whether automated and manual penetration testing was performed.**		
180	D.1.1	1. Check for the existence of a comprehensive network penetration testing policy and assess the regularity and comprehensiveness of penetration tests.			
181	D.1.2	2. Check the scope of penetration tests covers critical assets and network segments and assess if both automated and manual testing were conducted.			
182	**E**	**Network and Device Configuration Review**			
183	**E.1**	**Device Configuration Review**	**Perform configuration review of network and security devices in accordance with industry standards**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
			and security guidelines such CIS benchmark, NIST, etc.		
184	E.1.1	1. Check the access controls, encryption protocols, and authentication mechanisms for robust network security.			
185	E.1.2	2. Check the firewall rules, intrusion prevention systems, anti-malware and proper network segmentation.			
186	E.1.3	3. Check the VPN configuration and user accesses			
187	E.1.4	4. Check the wireless network configurations, remote management configurations and verify the use of strong, unique passwords and the absence of default credentials.			
188	E.1.5	5. Verify that only necessary services, protocols, and ports are allowed.			
189	E.1.6	6. Assess the use of role-based access controls (RBAC) for administrative access.			
190	E.1.7	7. Check network devices are running the latest firmware or software versions.			
191	E.1.8	8. Review SNMP configurations and ensure they use secure versions (e.g., SNMPv3). Implement strong community strings and restrict access to SNMP management.			
192	E.1.10	10. Verify syslog configurations for logging critical events.			
193	E.1.11	11. Verify network segmentation to contain and minimize the impact of potential breaches. Ensure that VLANs are appropriately configured and isolated.			
194	E.1.12	13. Check port security, Quality of Service (QoS) and Network Time Protocol (NTP) synchronization.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
195	**E.2**	**Network Redundancy**	**Review the network redundancy for single point of failures.** **Review whether the network redundancy tests were performed by organization to check the failover mechanism**		
196	E.2.1	1. Check the implementation of redundancy, failover mechanisms, and secure routing.			
197	**E.3**	**Logging and Monitoring**	**Review whether network logs are maintained and monitored by network operations team. Check for log retention and archival policy**		
198	E.3.1	1. Check for NOC reports			
199	E.3.2	2. Check for log retention and archival policy			
200	E.3.3	3. Review the configuration of Security Information and Event Management (SIEM) tools. Assess the performance and scalability of SIEM solutions to handle the volume of logs generated.			
201	E.3.4	5. Does Devices being used in reverse proxy mode such as WAF,LB have enabled requisite header format for web hosting. Ensure that Sensitive PII data is masked/hashed/encrypted.			
202	**F**	**Application Hosting Configuration Review**			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
203	**F.1**	**Hosting Environment Security**	**Review the hosting system security configurations for Applications and critical databases to determine the following: - Adherence to secure hosting standards, encompassing secure protocols, encryption, hosting platform/system access controls, authentication mechanisms, and proper segmentation for hosted applications and databases.** **- Application and Database hosting servers are segregated and access is established through zero trust mechanism.** **- Servers hosting critical databases is access controlled, is not accessible on internet.** **- Hosting systems are integrated with SOC/SIEM solutions and monitored for access and changes.**		
204	F.1.1	1. Check adherence to secure hosting standards, encompassing secure protocols, encryption, hosting platform/system access controls, authentication mechanisms, and proper segmentation for hosted applications.			
205	F.1.2	2. Check that Application and Database hosting servers are segregated and access is established through zero trust mechanism.			
206	F.1.3	3. Check that server hosting critical database / PII information is not accessible on internet. Check that user access to critical			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
		database / PII data / underlying servers is restricted to authorized users only. Privilege access is restricted and monitored.			
207	F.1.4	4. Check that Application Server and Critical Database Servers hosting PII information are integrated for security monitoring with SOC / SIEM solution. Check that access and transaction logs are secured and retained.			
208	F.1.5	5. Check that server hosting application and critical database is updated for latest security patches. Check that server hosting application, critical database, middleware and load-balancer etc. is hardened and benchmarked against security standards such as CIS.			
209	**F.2**	**Security Monitoring of Hosting Environment**	**Review whether hosting systems are integrated with SOC/SIEMsolutions and monitored for access and changes.** **Review whether effective security monitoring,** **and application isolation in case of virtualization is configured**		
210	F.2.1	1. Check the effectiveness of intrusion detection, monitoring, and logging mechanisms in the hosting environment.			
211	F.2.2	2. Check that hosting servers have antivirus/anti-malware and data loss protection software are installed and security threat signatures/definitions are updated.			
212	F.2.3	3. Check the security monitoring of hosted applications, databases and associated user access to servers / Operation System.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
213	F.2.4	4. Check the use of containerization or virtualization for secure application isolation.			
214	**F.3**	**Security Assurance on Third Party Cloud Service Provider (CSP)**	**In-case of applications and / or critical databases hosted on external / third party cloud service provider (CSP), review the hosting environment security assurance reports based on SOC2 Type 2 Examination issued to auditee organization by CSP, to determine the following:** **- Independent auditor opinion** **- management assertions / statement on CSP security control environment - security control deficiencies** **- user entity controls applicable for security governance and management by user organization / auditee organization**		
215	F.3.1	1. Check the CSP hosting environment SOC2 Type2 report for detailed security controls and their effectiveness status. Enquire with auditee management on controls that are ineffective or qualified by CSP's auditors in the SOC2 Type2 report and assess the compensating controls.			
216	**F.4**	**Backup and System Resilience**	**Review the data backup and archival process.** **Review whether backup testing was performed and its effectiveness**		

217	F.4.1	1. Check the data backup and archival policy and procedures and Check the backup testing reports			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
218	**F.5**	**Hosting System Decommissioning / Migration**	**Review the hosting system decommissioning / migration process. Determine how the data is securely erased (for decommissioning) / transferred during system migration.**		
219	F.5.1	1. Check for proper disposal and decommissioning processes for deprecated hosting resources / end-of-life servers.			
220	F.5.2	2. Confirm the use of encryption for data in transit (TLS/SSL) and data at rest (disk encryption). Assess the strength of encryption algorithms and key management practices.			
221	F.5.3	4. Review Identity and Access Management (IAM) configurations for users, groups, and roles.			
222	F.5.4	5. Assess access controls and permissions and ensure the use of multi-factor authentication (MFA)..			
223	F.5.5	7. Verify the security configurations of servers and workstations.			
224	F.5.6	8. Assess antivirus/antimalware solutions and their update status and Confirm secure configurations for endpoint protection.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
225	**G**	**Database Security Assessment**	**(including whether personal data is being encrypted at rest and in motion, or used in tokenized form, or obfuscated/masked; and whether the access privileges to the back-end data segment of the application are limited to the minimum necessary set of authorized users and are protected with multi-factor authentication)**		
226	**G.1**	**Access control, Authentication and Monitoring**	**Review the access management and monitoring controls, including multi-factor authentication (MFA) mechanism for secure access to critical database.**		
227	G.1.1	1. Check for access controls, encryption, monitoring mechanisms for database security and confirm secure configuration settings, including proper authentication methods and multi-factor authentication.			
228	**G2**	**Database Encryption**	**Review if the PII data information in database is encrypted.**		
229	G.2.1	1. Check the data base encryption configuration for protecting PII data.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
230	**G.3**	**Database Updates and Patch Management Review**	**Review the patch management process and update of security patches on database servers.**		
231	G.3.1	1. Check for regular reviews and updates of the database management system software. Check timely implementation of patches and updates for the database.			
232	**G4**	**Database Activity Monitoring**	**Review whether Database Activity Monitoring (DAM) tool is implemented to monitor user and privilege access to databases.** **Review the DAM rules to determine whether logics have been implemented to prevent privilege access escalation attacks.**		
233	G.4.1	1. Check for DAM implementation and its rule sets.			
234	**H**	**User Access Controls**	**including (privilege access management) and access reconciliation review**		
235	**H.1**	**User Access Management Policy and Controls**	**Review user access controls, access management policies and mechanism that are implemented for access to applications, databases, hosting environment (operating system), active directory / LDAP, network devices and security equipment.**		
236	H.1.1	1. Check existence and effectiveness of documented user access control policies, user authentication mechanisms and adherence to strong password policies.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
237	H.1.2	2. Check for periodic user access reviews performed by management. Verify if user access were revoked in timely manner for terminated or inactive users.			
238	**H.2**	**Privileged user controls and Segregation of Duties / Roles**	**Review whether the privileged accounts are protected and segregation of duties has been defined**		
239	H.2.1	1. Check for role-based access controls, use of multi-factor authentication and verify proper segregation of duties and implementation of least privilege principles.			
240	H.2.2	2. Check the implementation of account lockout mechanisms and privileged access controls.			
241	**H.3**	**User Credentials Management**	**Review the management and storage of users credentials.**		
242	H.3.1	1. Check for secure storage, transmission, and recovery of user credentials. Check the password management policy and how it is enforced in system. Check whether user credentials are not stored in clear text.			
243	**I**	**Identity and Access Management (IAM) Controls Review**			

244	**I.1**	**IAM Policy, Procedure and Access controls**	**Review the existence and effectiveness of IAM policy and procedures.** **Review whether IAM, PIM/PAM tool is integrated for applications, databases and other hosting system components. Review whether workflow is defined for IAM tool for user access approval.**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
245	I.1.1	1. Check for integration and use of IAM/PIM/PAM tool for user access management.			
246	I.1.2	2. Check for privileged access management controls, regular policy updates and check documentation, communication, and monitoring of IAM policies and activities.			
247	**I.2**	**IAM Security Controls and Authentication Mechanism**	**Review the authentication mechanism and third-party access controls on IAM tool.**		
248	I.2.1	1. Check for the use of Single Sign-On (SSO) and multi-factor authentication and evaluate encryption methods for IAM data and credentials.			
249	I.2.2	2. Check for IAM controls for third-party access, cloud applications, and integrations.			
250	**J**	**Data Protection Controls Review**	**(inter alia, with reference to advisories issued by CERT-In from time to time regarding prevention of data leaks, including "Preventing Data Breaches / Data Leaks [CIAD-2021-0004]")**		
251	**J.1**	**Data Protection Policies**	**Review the Data Protection Policies and Procedures in place to identify and protect PII / Critical Data in the auditee organization.** **Review if PII Data Flow is documented.** **Review if the Data Protection Impact Assessment (DPIA) has been performed by auditee organization.**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
252	J.1.1	1. Check for Data Protection Policies and Procedures.			
253	J.1.2	2. Check where data flow and data classification has been performed to identify and protect critical / PII data.			
254	J.1.3	3. Check whether data protection impact assessment (DPIA) has been performed to assess the impact to organisation in event of data loss / leakage.			
255	J.1.4	4. Evaluate mechanisms for obtaining user consent for data storage and usage. (as per DPDP Act 2023)			
256	J.1.5	5. Organizations must ensure that individuals provide informed consent for the processing of their personal data. This means individuals should be aware of the purposes for which their data is being processed			
257	**J.2**	**DLP Tools Implementation**	**Review whether DLP tool has been implemented for all critical data assets and systems.**		
258	J.2.1	1. Check for comprehensive coverage of DLP tool implementation. . Check the DLP reports and incidents reports for efficacy of DLP rules.			
259	**J.3**	**Data Storage and Encryption Review**	**Review the data encryption implementation for data at rest (in database) and data in motion (network)**		
260	J.3.1	1. Check for encrypted storage and transmission of critical / personal data / PII data. . Check the encryption and security measures for data transferred to third parties.			
261	J.3.2	3. Ensure that encryption standards used for data storage align with industry best practices and legal requirements. Utilize strong encryption algorithms for both data in transit and data at rest.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
262	J.3.3	5. Review and enforce access controls to restrict unauthorized access to personal data.			
263	J.3.4	6. Implement the principle of least privilege, ensuring individuals have access only to the data necessary for their role.			
264	J.3.5	7. Confirm that personal data is stored in locations compliant with data protection laws. Be aware of restrictions on cross-border data transfers and ensure compliance with those regulations.			
265	J.3.6	8. Review and document data retention policies.			
266	J.3.7	9. Implement procedures for the secure disposal/archival of personal data that is no longer needed.			
267	J.3.8	10. Ensure that Sensitive PII data is masked/hashed/encrypted.			
268	**K**	**Security Operations and Monitoring Review**	**including maintenance of security logs, correlation and analysis**		
269	**K.1**	**Security Operations and Monitoring Policy**	**Review Security Operations Center (SOC) policy and procedures**		
270	K.1.1	1. Check for existence and effectiveness of security operations, monitoring policy, vulnerability management process, and incident response plans.			
271	K.1.2	2. Check if SOC monitors network and endpoint security controls, including privileged user monitoring and check for conduct of incident reports and periodic security drills.			
272	**K.2**	**SOC monitoring for Incidents**	**Review SOC/SIEM coverage for devices integration, log correlations and security incident alert notifications.**		
273	K.2.1	1. Check for SOC/ SIEM utilization for log management and analysis. Check the SOC/ SIEM correlation rules and check if they adequately cover the security requirements.			

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
274	K.2.2	2. Check for the device coverage and number of devices integrated with the SIEM solution.			
275	**K.3**	**Security Monitoring, Orchestration, and Analytics**	**Review SOC effectiveness and efficiency to detect threats, patterns & anomalies using automation, orchestration, and threat intelligence**		
276	K.3.1	1. Check for the effectiveness of the security operations center (SOC) and use of security automation, orchestration tools, access controls, sensitive data monitoring, and documentation of procedures.			
277	K.3.2	2. Check for integration and availability of threat feeds in SOC. Check if SOC team performs security analytics for anomaly detection.			
278	**L**	**Review of logs, backup and archival data for access to personal data**	**(including whether personal data not in use / functionally required is available online rather than archived offline; and whether logs of all its ICT systems are maintained securely within Indian jurisdiction for a rolling period of 180 days, or such other period as CERT-In may require through directions issued by it in exercise of powers vested in it by law)**		
279	**L.1**	**Log management and backup policies**	**Review the application transaction and security log management process**		

Sl. No.	Control No.	Domain	Controls & Review Guidelines to Auditor / Reviewer	Compliance (Yes / No / NA)	Remarks
280	L.1.1	1. Check for existence and effectiveness of application transaction and security logs.			
281	**L.2**	**Log Backup, Retention and Archival**	**Review the log backup/retention and archival process**		
282	L.2.1	1. Check for backup and retention policies and archival procedures.			

****

Schedule of Quantities

(Tender/Bid ID: GEM/2024/B/4926424)

Name of Work-: "Design, Development, Launching, Maintenance and associated services of e-Internship portal".

(Amount in Indian National Rupees)

Schedule of Quantities						
Name of Work: Design, Development, Launching, Maintenance and associated services of e-Internship portal						
Instructions: All yellow cells only need to be filled .						
Payment terms: 40% of the total cost (Sl. no 4 of this BOQ) will be paid after the design, development & launching of Internship portal and successful completion of acceptance test. 7.5% of the total cost (Sl. no 4 of this BOQ) will be paid quarterly in equal installement for eight quarter for the cost of hosting, maintenance and associated services And first quarterly payment will be made after three months from the final user acceptance test. 8.5% of the quarterly charges will be paid additionally for the usage charges for every additional users in the multiples of 200 and/or every additional certificates in the multiples of 2000 will be paid						
S.N.	Item Description	Quantity	Units	GST in %	Basic rate in figures (Price in INR Including GST)	Total amount(Price in INR including GST)
1	Design, Development and launching cost of Internship portal as per scope of work	1	Lot			₹ 0.00
2	Hosting cost to cater the users up to 600 and Digital certificates up to 6000 per annum as per the scope of work	24	Months			₹ 0.00
3	Maintenance & Service cost to cater the users up to 600 and Digital certificates up to 6000 per annum as per the scope of work.	24	Months			₹ 0.00
4	Total cost for the design, development, launching of the Internship portal, hosting, maintenance, and associated services for 24 months to cater the users up to 600 and Digital certificates up to 6000 per annum as per the scope of work.					₹ 0.00

Note 1: Financial bid comparison shall be done on the basis of Grand total cost.

Note 2: Only one financial bid is to be submitted by one vendor.

PAGE LEFT BLANK

INTENTIONALLY