

REQUEST FOR EXPRESSION OF INTEREST (REOI)

HIRING OF SHORT-TERM CONSULTANCY FIRM FOR ISO STANDARDS (PREFERABLY ISO 27001)"

Punjab Safe Cities Authority (PSCA), established under Punjab Safe Cities Act 2016, ensures establishment, development and maintenance of an Integrated Command, Control, and Communication system for Police in major cities of the province for public safety. The Safe City is a concept for returning security and quality of life to today's complex cities through the use of technology, infrastructure, personnel and processes.

2. PSCA intends to hire services of a qualified, well experienced and competent Consultancy Firm for the **Implementation of ISMS and Acquisition of ISO-27001 Certification**. The Consultancy Firm shall provide services in accordance with the Terms of Reference (TORs) (**Annex-A**). The Consultancy Firm shall be hired on the basis of qualification and experience in accordance with Rule 46 (*Selection process of individual consultant- in a short consultancy*) read with Rule 45(2) of the Punjab Procurement Rules, 2014.
3. Interested Consultancy Firm should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services. The detailed Terms of Reference are attached as **Annex-A**. The technical evaluation criteria (Mandatory Requirements) is attached as **Annexure-B**. The Financial Bid Performa is attached at **Annex-C**.
4. Technical (Mandatory Documents) & Financial Quotations along with all the supporting documents shall be submitted on or before **April 25, 2025** till **1600 hours** through **ePAD**. Expression of Interests will be opened on the **same date** at **1630 hours** in the presence of bidders who may choose to attend with original CNIC.
5. For obtaining any further information or clarifications, please feel free to contact during office hours 0900 to 1600 (Monday to Friday) at procurement@psc.gov.pk, Tel: (+92) (42) (99051605-7) Ext: 2521.

(CHIEF LAW & PROCUREMENT OFFICER)
PUNJAB SAFE CITIES AUTHORITY,
Lahore

Annex-A

TERMS OF REFERENCE “CONSULTING SERVICES FOR ISO STANDARDS (PREFERABLY ISO 27001)”

1. BACKGROUND

With reference to the subject matter, it is to inform that an ISMS helps organizations safeguard sensitive data, including customer information, financial records, intellectual property, and proprietary business processes. By systematically managing and securing this data, an ISMS reduces the risk of data breaches, theft, or unauthorized access. It also helps identify, assess, and manage security risks systematically. By conducting regular risk assessments, organizations can proactively address vulnerabilities and minimize the potential impact of cyber-attacks, natural disasters, or human errors. A strong security posture enhances the organization's reputation and can be a competitive advantage, especially in industries where privacy and security are critical.

An ISMS ensures the continuity of business operations even in the face of unexpected security incidents or breaches. By establishing effective recovery processes and contingency plans, the organization can reduce downtime and ensure rapid recovery from disruptions. With the rise in cyber threats such as ransom ware, phishing, and data breaches, an ISMS provides a structured approach to safeguarding IT systems and networks. It ensures that security controls are in place to protect against a wide range of cyber-attacks.

The implementation of an ISMS provides management with clear insights into the organization's information security posture, facilitating better decision-making. It also ensures that governance structures are in place to oversee the security efforts, define roles, and allocate resources effectively.

ISO-27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). The goal of the standard is to help organizations protect their information assets systematically and effectively through the implementation of policies, procedures, and controls.

2. OBJECTIVE/PURPOSE OF THE ASSIGNMENT

The selected Consultancy Firm will provide complete consulting services required for development and implementation of information security management system based on ISO 27001 and support in achievement of its certification.

3. SCOPE OF SERVICE

- Gap Analysis against requirements of ISO 27001 and report submission (For PSCA Main Office as well as DR Site)
- Comprehensive Project Plan (to be achieved within a period of 16 weeks)
- Documentation plan for ISMS Policies and Procedures based on findings of Gap Analysis
- ISMS Policies and Procedures customized and delivered as per requirements of PSCA
- Statement of Applicability as per the controls adopted by PSCA
- Comprehensive Risk management based on the controls adopted by PSCA (and also guide in implementation of any missing controls)
- Service/Business Continuity Plan for the Scope of ISMS
- Internal Audit planning and execution
- Internal Audit reporting and corrective action planning
- Supporting in Certification Body Selection
- Support services in Stage-1 and Stage 2 Audits by Certification Body
- Ensuring clearance of PSCA during Certification Audit (including support required for corrective actions as per Auditor's recommendations)

4. PROFILE OF INDIVIDUAL CONSULTANT

- Firm must be registered at EPAD
- Firm must have overall experience of 5 years or higher in ISO consulting services (FBR or Chamber of Commerce registration evidence required)
- Firm must have experience of ISO 27001 consulting services (Evidence of at least 3 similar assignments of ISO 27001 required)

6. PROJECT MANAGER CRITERIA:

- The Project Manager (Lead Consultant) representing the firm, is required to have at least 10 years of experience in information security and relevant IT related ISO standards' consultancy and auditing (such as Information security, business continuity, IT services management, etc.).
- The Project Manager must have completed course on LA/LI ISO 27001.

7. EXPECTED DELIVERABLES

- Gap Analysis Report
- Project Plan
- Finalization of ISMS Scope
- ISMS Documentation Plan
- ISMS Policies and Procedures
- Statement of Applicability (SOA)
- Risk Management document (Risk Assessment and Treatment Plan)
- Service/Business Continuity Plan for Scope of ISMS
- Internal Audit Plan
- Internal Audit Report and Corrective Action Plan
- Project Status Sheet (weekly update on project status)

8. TIME PERIOD

The Consultancy Firm will be engaged for a period as desired by Competent Authority.

9. PAYMENT TO THE CONSULTANT

The Payment schedule will be made as per the following milestones after issuance of satisfactory note by the Focal person/Concerned Unit Head of PSCA:

SN	DELIVERABLES	PERCENTAGE
1.	<ul style="list-style-type: none">• Gap Analysis Report	20%
2.	<ul style="list-style-type: none">• Project Plan• Finalization of ISMS Scope• ISMS Documentation Plan• ISMS Policies and Procedures• Statement of Applicability (SOA)	40%

3.	<ul style="list-style-type: none">• Risk Management document (Risk Assessment and Treatment Plan)• Business Continuity Plan for the Scope of ISMS• Internal Audit Plan• Internal Audit Report and Corrective Action Plan• Recommendation Letter by Certification Body for ISO 27001	40%
----	---	-----

Annex-B

8. MANDATORY REQUIREMENT

Following criteria shall be followed to evaluate the most suitable firm for the assignment:

Sr.#	Description	Yes/No
1.	Copy of Valid Income Tax Registration (NTN) (signed & stamped)	
2.	Copy of valid Punjab Sales Tax (GST/PST) (signed & stamped)	
3.	Affidavit on non-Judicial E-Stamper of PKR. 100/- (signed & stamped)	
EXPERIENCE		
4.	Firm must have overall experience of 5 years or higher in ISO consulting services	
5.	Firm must have experience of ISO 27001 consulting services (Evidence of at least 3 similar assignments of ISO 27001 required)	
PROJECT MANAGER CRITERIA:		
6.	The Project Manager (Lead Consultant) representing the firm, is required to have at least 10 years of experience in information security and relevant IT related ISO standards' consultancy and auditing (such as Information security, business continuity, IT services management, etc.).	
7.	The Project Manager must have completed course on LA/LI ISO 27001.	

8.	Signed & stamped TORs	
----	-----------------------	--

Note:

1. The Consultancy Firm shall be declared **Lowest Evaluated** if it **qualified Evaluation Criteria: Mandatory Requirements)**” and **lowest financially** subject to fulfilment of all other terms & conditions.
2. All documents must be signed & stamped.

ANNEX-C

9. FINANCIAL BID PERFORMA

Sr.#	Description	Total Price PKR (Inclusive of all applicable taxes)	
		Estimated Price	Quoted Price
1.	Consultancy Fee for “Hiring of short-term Consultancy Services for implementation of ISMS and acquisition of ISO-27001 certification”	900,000/-	

Total Price PKR (Inclusive of all applicable Taxes) in Words: -----

Note:

1. The Consultancy Firm shall be declared **Lowest Evaluated** if it **qualified** **Evaluation Criteria: Mandatory Requirements** and **lowest financially** subject to fulfilment of all other terms & conditions.
2. A lump-sum price (inclusive of all applicable taxes) shall be calculated to financially evaluate the bid. However, each column above is requested to be filled against each city.
3. **Least Cost Selection Method** shall be adopted to evaluate the financial proposal.
4. The firm/company is required to complete the price schedule carefully and in case of any discrepancy or multiple price the bid shall not be considered.
5. In case of difference between amount in “words” and amount in “figures”, amount in “words” shall be considered final.
6. Alternative or other than this Performa or incomplete Performa shall not be acceptable.

ANNEX-D

AFFIDAVIT

*[To be printed on **PKR. 100/- E-Stamp Paper**, duly attested by oath commissioner. To be attached with Technical Bid]*

Name: _____ *(Applicant)*

I, the undersigned, do hereby certify that all the statements made in the Bidding document and in the supporting documents are true, correct and valid to the best of my knowledge and belief and may be verified by employer if the Employer, at any time, deems it necessary.

The undersigned hereby authorize and request the bank, person, company or corporation to furnish any additional information requested by the **Punjab Safe Cities Authority** of the Punjab deemed necessary to verify this statement regarding my (our) competence and general reputation.

The undersigned understands and agrees that further qualifying information may be requested and agrees to furnish any such information at the request of the **Punjab Safe Cities Authority**. The undersigned further affirms on behalf of the firm that:

- (i) The firm is not currently blacklisted by the Procuring Agency.
- (ii) The documents/photocopies provided with Bid are authentic. In case, any fake/bogus document was found at any stage, the firm shall be blacklisted as per Law/ Rules.
- (iii) The provided information is correct.

Signed by an authorized Officer of the company

Title of Officer: _____

Name of Company: _____

Date: _____

ANNEX-E

NON-DISCLOSURE AGREEMENT (NDA)- SAMPLE

This Non-Disclosure Agreement (**the "Agreement"**) is made and entered into as of -
---- **day of -----, 2025** by and between:

Punjab Safe Cities Authority (PSCA), Government of Punjab, duly established under the PSCA, Act 2016, having its headquarters at PPIC3 Centre, Qurban Lines, Jail Road, Lahore, Punjab/Pakistan, (hereinafter referred to as the "**Disclosing Party**" which expression shall include its successors-in-interest and permitted assigns;

AND

[Consultant Name], an Individual Consultant, located at -----
-----, (hereinafter referred to as the "**Receiving Party**" which expression shall include its successors-in-interest and permitted assignees).

WHEREAS, the Disclosing Party intends to disclose certain confidential and proprietary information (the "Confidential Information") to the Receiving Party for the purpose of engaging the Receiving Party for the Provision of consultancy services (the "Services").

NOW, THEREFORE, in consideration of the mutual promises herein contained, the parties agree as follows:

1. CONFIDENTIAL INFORMATION

For purposes of this Agreement, "Confidential Information" shall include but is not limited to, all written, oral, or electronic information, documentation, reports, designs, data, software, business plans, trade secrets, marketing strategies, customer information, proprietary methodologies, IT systems and any other materials related to the Disclosing Party and IT systems disclosed to the Receiving Party, whether marked as confidential or not.

2. OBLIGATIONS OF THE RECEIVING PARTY

The Receiving Party agrees to:

- 2.1. **Confidentiality:** Maintain the highest level of confidentiality with respect to all Confidential Information disclosed by the Disclosing Party. The Receiving Party shall not, without the prior written consent of the Disclosing Party, disclose, share, publish, or otherwise use any Confidential Information for any purpose other than the specific purpose of providing the Services under this Agreement. The Receiving Party shall take all reasonable and necessary measures to safeguard the Confidential

Information and prevent any unauthorized access, disclosure, or use, including but not limited to, implementing appropriate security protocols.

- 2.2. **Non-Disclosure:** The Receiving Party agrees not to disclose any Confidential Information to any third party without the prior written consent of the Disclosing Party. This obligation shall continue indefinitely, including after the termination of this Agreement and shall continue regardless of whether the Confidential Information remains in the possession of the Receiving Party or has been returned or destroyed.
- 2.3. **Limited Access:** The Receiving Party shall not disclose Confidential Information to any individuals within their organization, except those who have a direct need to know for the sole purpose of fulfilling the Services, and who are bound by written obligations of confidentiality that are at least as restrictive as the terms of this Agreement. The Receiving Party shall ensure that any such individuals are informed of the confidential nature of the information and comply fully with the confidentiality obligations set forth herein.
- 2.4. **No Reverse Engineering:** The Receiving Party acknowledges that all software, systems, and related intellectual property disclosed by the Disclosing Party, including but not limited to source code, underlying ideas, algorithms, designs, and documentation, are proprietary and confidential. The Receiving Party shall not, directly or indirectly, reverse engineer, disassemble, decompile, decode, or otherwise attempt to derive or reconstruct the source code, underlying structure, ideas, or algorithms of any part of the Disclosing Party's software, systems, or technology, nor shall the Receiving Party assist or permit any third party to do so. This prohibition shall apply regardless of whether such activities are for commercial or non-commercial purposes and shall continue indefinitely, including after the termination of this Agreement.

3. EXCLUSIONS FROM CONFIDENTIAL INFORMATION

Confidential Information shall not include information that:

- i. Becomes publicly available through no breach of this Agreement by the Receiving Party.
- ii. received from a third party without breach of any obligation of confidentiality, provided that the Receiving Party can demonstrate, to the satisfaction of the Disclosing Party, that the third party had the lawful right to disclose such information.
- iii. Independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information, but only if the Receiving Party can provide clear and convincing evidence that such independent development was done without reliance on any Confidential Information provided by the Disclosing Party.

4. TERM

This Agreement shall commence on the Effective date and shall continue in effect

until the Confidential Information no longer qualifies as confidential or until terminated by either party with thirty (30) days written notice to the other party.

5. RETURN OF MATERIALS

Upon termination of this Agreement, or at any time upon the Disclosing Party's request, the Receiving Party shall immediately return to the Disclosing Party, or at the Disclosing Party's sole discretion, destroy all materials containing Confidential Information, including all copies, reproductions, summaries, or any other form of Confidential Information in the Receiving Party's possession. The Receiving Party shall provide written certification to the Disclosing Party within a specified period, as determined by the Disclosing Party, confirming full compliance with this obligation, including a detailed account of the actions taken to return or destroy all Confidential Information.

6. NO LICENSE

Nothing in this Agreement shall be construed as granting the Receiving Party any license, right, title, or interest in or to the Confidential Information, whether by implication, estoppel, or otherwise, except for the limited right to use the Confidential Information solely for the purpose of performing the Services under this Agreement. The Receiving Party agrees that it will not, directly or indirectly, use, copy, reproduce, modify, distribute, or otherwise exploit any Confidential Information for any purpose other than as expressly permitted in this Agreement. All rights in and to the Confidential Information shall remain solely with the Disclosing Party, and the Receiving Party shall have no rights whatsoever to use or disclose such information beyond the express terms set forth herein.

7. GOVERNING LAW

This Agreement shall be governed by and construed in accordance with the laws of the Punjab, Pakistan.

8. MISCELLANEOUS

- 8.1. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior discussions or agreements.
- 8.2. No modification or amendment of this Agreement shall be effective unless in writing and signed by both parties.
- 8.3. In the event of any breach of confidentiality or non-disclosure of data, the undersigned shall be held fully responsible for any damages, losses, or penalties incurred by the Disclosing Party. Furthermore, the Disclosing Party shall have the exclusive right to determine the amount of such damages or penalties, and the undersigned shall promptly pay the full amount as



determined by the Disclosing Party. In addition, the Disclosing Party reserves the unequivocal right to initiate legal proceedings as per applicable laws against the undersigned in Court of Competent Jurisdiction, and in such cases, the undersigned shall be solely responsible for all legal costs, attorney fees, and any other expenses incurred by the Disclosing Party in connection with the legal proceedings. The undersigned shall also indemnify and hold harmless the Disclosing Party for any further claims or losses resulting from the breach. I have read and understood the above contents and accepted/signed the same without any duress, undue influence or pressure, coercion and with my free consent.

9. SIGNATURES

By signing below, the parties acknowledge that they have read, understand, and agree to be bound by the terms of this Agreement.

**Punjab Safe Cities Authority
(Disclosing Party)**

Name: _____

Designation: _____

Signatures: _____

**[Consultancy Firm's Name] (Receiving
Party)**

Name: _____

Designation: _____

Signatures: _____

Witness (1)

Name: _____

Designation: _____

Signatures: _____

Witness (2)

Name: _____

Designation: _____

Signatures: _____