REQUEST FOR EXPRESSIONS OF INTEREST (CONSULTING SERVICES – FIRMS SELECTION)

[HIGHER EDUCATION DEVELOPMENT IN PAKISTAN (HEDP) PROJECT]

Credit No: 6438

Assignment Title: Consultancy for Updating the Policy Framework for ICT and Cybersecurity**.**

Reference No.: PK-HEC-256560-CS-CQS

The Higher Education Commission ("HEC") has *received* financing from the World Bank (WB) toward the higher education development in Pakistan (HEDP) and intends to apply part of the proceeds for consulting services.

The consulting services ("the Services") includes preparation of Policy Framework for ICT and Cybersecurity

The detailed Terms of Reference (TOR) for the assignment *are attached to this request for expressions of interest and can be downloaded from: www.hec.gov.pk.*

The Higher Education Commission now invites eligible consulting firms ("Consultants") to indicate their interest in providing the Services. Interested Consultants should provide information demonstrating that they have the required qualifications and relevant experience to perform the Services as follows:

1. At least Ten (10) years of post-registration experience in any the fields of (i) ICT Policy Framework Development and drafting of relevant laws, (ii) Cybersecurity iv) IT System Review and Audits (v) Review/Development of Data Protection Policies in the public or private sector organizations.
2. Must demonstrate availability of key professionals in each area of assignment.
3. Must have adequate human and physical resources to support the consultancy with demonstrable documentary evidence.

The attention of interested consulting firms is drawn to Section III, paragraphs, 3.14, 3.16, and 3.17 of the World Bank's "Procurement Regulations for IPF Borrowers" July 2016 ("Procurement Regulations"), setting forth the World Bank's policy on conflict of interest.

A Consulting firms will be selected in accordance with the Consultant's Qualification-based Selection (CQS) method set out in the Procurement Regulations of the World Bank for IPF Borrower July 2016 Revised November 2017 and August 2018.

Further information can be obtained at the address below during office hours *i.e. 1000 to 1600 hours*.

Expressions of interest must be delivered in a written form to the address below (in person, or by mail, or by fax, or by e-mail) by **Nov 2, 2021.**

Muhammad Farooq Azam

Procurement Specialist

Higher Education Development in Pakistan (HEDP) - Project

Higher Education Commission, H-9, Islamabad

Tel: 051-90402806

Fax: 051-90402202

Email: mfazam@hec.gov.pk

Terms of Reference (TORs)

Consultancy for Updating the Policy Framework for ICT and Cybersecurity

Title:	**Consultancy for Updating the Policy Framework for ICT and Cybersecurity**
Category:	Consulting Services
Type of Contract:	Lumpsum
Expected Start Date:	December 2021
Duration of Assignment:	Six Months Contract
Selection Method	CQS

Background

To address the challenges of higher education in the country, the Government of Pakistan established Higher Education Commission (HEC) in 2002 with the mandate to reform and expend the higher education sector and to make Higher Education Institutes (HEIs) more relevant in the 21st century.

The "Higher Education Development in Pakistan (HEDP) Project is financed by the World Bank and aims to support the HEC's Vision 2025. The Development Objective(s) of the HEDP project include quipping Students and Higher Education Institutions with Modern Technology.

As HEC embraces technology to enable learning and collaboration, it has to accelerate the adoption of latest IT solutions, cloud-based services and support for mobile applications. HEC is also deploying a wide range of Internet-of-Things (IoT) devices as part of smart campus initiatives including but not limited to PERN, Eduroam, Smart Classrooms, Higher Education Data Repository (HEDR) and MOOCs. With the influx of these new technologies, comes an increased risk to network security, intellectual property and personal data. HEC collects a large amount of student and faculty data of the Public and Private Sector Universities and HEC also provides a number of IT services to these HEIs

1. Objectives of the Assignment

HEC intends to review its ICT Framework with a detailed assessment of its current IT Systems and a broad, integrated, and automated security platform the gives the HEC management a visibility

into their entire IT security infrastructure, both on HEC offices and across cloud deployments. HEC also intends to deploy robust analytical tools and controls to protect ever-evolving higher education networks and its users from all kinds of cyber threats.

2. Scope of Work

The Consulting Firm Will.

1. Review existing HEC ICT Framework and relevant ICT policies and procedures with the intention to update them as per the current and future needs
2. Based on review of national and international good practices and experiences, develop a HEC ICT Policy Framework as per the guidelines of Pakistan's National Cyber Security Policy 2021. The ICT policy will cover:
    - An overview of current IT services being provided by PERN to institutions and how these services may be enhanced
    - Improving HEC services to students and graduates
    - Strengthening of HEC internal IT architecture
    - HEC internal data structures and processes
    - Cybersecurity of HEC's IT architecture
    - Functional review of HEC's HR supporting IT services and capacity building needs

In developing the policy, the consulting firm will:

1. Benchmarking of HEC / PERN IT architecture and cybersecurity system with best practices from select top-of-class higher education institutes of NRENs in other countries, e.g. Sri Lanka, Bangladesh, and Europe.
2. [1]Review and recommend changes into the draft data protection policy considering the comments received from the stakeholders on the draft policy.
3. Undertake a forensic analysis to identify key security challenges for Higher Education Commission and HEIs in general, the volume, speed, and sophistication of new cyber threats, their probability and frequency. This can include both external and insider threats to users, campus infrastructure, associated data centers and high value assets.
4. Review software and hardware being utilized to store, access, and transmit both valuable research data and encrypt sensitive personally identifiable information (PII) using Cloud and HEC-PERN networks.

[1] Students and faculty personal data and educational records are protected by Draft Data Protection Policy

5. Recommend a broad, integrated, and automated security platform that gives visibility into the entire security infrastructure, both on and off HEC campus and across cloud deployments.
6. Recommend robust state of the art analytical tools, techniques and controls to detect cyber-attacks and mitigating their impact in case of breaches with a view to protect ever-evolving higher education networks and supports different use cases, including threat notification, warning notification, incident reporting and continuous diagnostic monitoring
7. Review and recommend systems for HEC to accepts credit card/online payments for its services, which must comply with the Payment Card Industry Data Security Standard (PCI DSS).
8. Review and recommend software tools, to provide Endpoint Recovery Services by delivering the right combination of technology, intelligence and expertise to assist HEC, with the detection, analysis and remediation of known security incidents and enable rapid recovery with minimal business interruption.
9. Review and recommend software tools for Network Security Monitoring capability for detection, response and threat hunting against unauthorized access, exposure or exploitation
10. Review current HEC ICT framework and develop detailed plans for implementation of ISO/IEC 27001 standards at HEC.
11. Develop data backup policies, data retention policies, disaster recovery plans, policies and recommendations for DR platforms.
12. Develop a Short and Medium - Term resource requirement plan, with detailed Job Descriptors of Proposed New Positions, Financial and HR requirement for HEC to implement and sustain the systems in long term
13. Capacity building recommendations including cybersecurity training for those with significant security responsibility and developing capacity of staff for HEC IT to implement the new ICT Framework and allied IT systems.
14. Any other item that the consultant deems necessary for this purpose.

3. Duration and Key Deliverables

Deliverable	**Timeline**
Inception Report	Two Weeks after Contract Signing
Desk Review of Existing HEC and National ICT Policies and Frameworks (Including Draft HEC Data Protection Policy) Covering bullet 1-4	Six Weeks after Signing of Contracts

A consolidated Mapping/Review and recommendation Report covering bullet points 5-6	Ten Weeks after Signing of Contracts
A consolidated Review and Recommendation for HEC to accepts credit card/Online payments covering bullet 7	Fourteen Weeks after Signing of Contracts
A consolidated Review and Recommendation Report covering bullet points 8-11, and detailed implementation plan for ISO 27001 certification of HEC	Eighteen Weeks after Signing of Contracts
A consolidated Review and Development of Plans covering bullet points 12-14	Twenty Two Weeks after Signing of Contracts
Consolidated Review and Implementation Plan	Twenty Six weeks after contract signing
Training to the HEC employees on the implementation of the relevant standards and updated policies as well as support the implementation of relevant standards and policies	Start after "A consolidated Review and Development of Plans covering bullet points 12-14" has been completed.

4. Qualifications/Shortlisting Criteria of the Consulting Firm

1. At least Ten (10) years of post-registration experience in any the fields of (i) ICT Policy Framework Development and drafting of relevant laws, (ii) Cybersecurity iv) IT System Review and Audits (v) Review/Development of Data Protection Policies in the public or private sector organizations
2. Must demonstrate availability of key professionals in each area of assignment.
3. Must have adequate human and physical resources to support the consultancy with demonstrable documentary evidence.

Key professionals of Consultant Firm

The firm must have a strong team including ICT legal experts, Data Privacy and Cybersecurity Experts, Financial Integration Experts, ISO 27001 Certification experts and auditors or equivalent, five (05) years post qualification experience in the relevant fields.

Key Professionals:

- ICT Legal Framework Expert/ Team Lead (16 Years of Education with 10 years of experience in ICT Legal Framework at National and International organizations)
- Data Privacy and Cyber Security Expert (16 Years of Education with 05 years of experience in cyber security and data privacy at International Organizations)

- ISO 27001 Certification Expert (16 Years of Education with 05 years of experience in either ISO 27001 Audit or Implementation standards)
- Financial Integration Experts (16 Years of Education with 05 years of experience in Financial Integration at National Organizations)

5. SELECTION PROCESS

A consulting firm will be selected in accordance with Consultant's Qualification Based Selection method set out in the "World Bank Procurement Regulations for IPF Borrowers (July 2016) Revised November 2017 & August 2018 www.worldbank.org/procure.