# INVITATION FOR PRE-QUALIFICATION OF FIRMS/ SERVICE PROVIDERS FOR CYBER SECURITY-RELATED SERVICES AND SOLUTIONS THROUGH OPEN FRAMEWORK AGREEMENTS


**National Electric Power Regulatory Authority**
**NEPRA Tower, Attaturk Avenue (East)**
**G-5/1, Islamabad**
**Phone No: 051-2013200 Fax: 051-9210215**
**www.nepra.org.pk**



NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

# National Electric Power Regulatory Authority
# NEPRA

**Tender No._____**

## INVITATION FOR PRE-QUALIFICATION OF FIRMS/ SERVICE PROVIDERS FOR CYBER SECURITY-RELATED SERVICES AND SOLUTIONS THROUGH OPEN FRAMEWORK AGREEMENTS

National Electric Power Regulatory Authority (NEPRA), a statutory body constituted under Act of Parliament (XL of 1997) to regulate the provisions of electric power sector, invites applications from the Cyber security firms/service providers for Cyber security related solutions and services through Open Framework Agreement(s) having set up at Rawalpindi/Islamabad and are:

i. Registered with Income Tax /Sales Tax Departments.
ii. In active taxpayers' list of the FBR.
iii. Having minimum six (06) years relevant experience.
iv. Not blacklisted in the public/private sector in Pakistan or abroad.

2. Pre-qualification documents, containing detailed terms and conditions are available for the interested parties at the office of the Assistant Director (Administration), NEPRA Tower, G-5/1 Islamabad.

3. Only the pre-qualified firms shall be entitled to participate in providing the cyber security services and solutions after signing the open framework Agreement(s) with the NEPRA for a period of three years, and the invitation to bids will be sent to the Pre-qualified applicants only.

4. The proposals, prepared in accordance with the instructions in the prequalification documents, must be submitted through E-Pak acquisition and Disposal System i.e. e-PAD on or before 6th day of May, 2024 @ 1400 hours. The proposals will be opened on the same day at 1430 hours. This advertisement and necessary tender documents are also available on NEPRA & PPRA websites at www.nepra.org.pk/tenders and www.ppra.org.pk respectively and may be downloaded free of cost.

**Director General (Administration/HR)**
**NEPRA Tower, Attaturk Avenue (East), G-5/1, Islamabad**
**PABX: +92 51 2013200, Fax: 051-9210215,**
**www.nepra.org.pk, info@nepra.org.pk**

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

# SECTION - I

## Schedule to Tender

| Sr.No | Activity Description | Schedule |
|---|---|---|
| 1. | Tender No. | No. /2024 |
| 2. | Sale of Pre-Qualification Document (PQD) | 30th March, 2024 to 6th May, 2024<br>Pre-Qualification document can be collected from the office of Assistant Director (Admin), NEPRA or downloaded from PPRA / NEPRA websites free of cost. |
| 3. | Time & Last Date of Depositing Tender | 6th May, 2024 upto 1400 hrs |
| 4. | Pre-Qualification Meeting | 23rd April, 2024 upto 1430 hrs<br>The queries must be submitted in writing via e-mail at the following email addresses given below:<br>Director (IT),<br>qain@nepra.org.pk<br>Deputy Director (Admin),<br>asfandyar@nepra.org.pk<br>Please include the following reference as the subject of your email:<br>"Firm/Service Providers for Cyber Security related Services and Solutions" |
| 5. | Time& Date of Opening of Tender Bid | 6th May, 2024 at 1430 hrs |
| 6. | Services to be Offered | Cyber security related Services & Solutions |
| 7. | Period of Contract | 3 years from the date of award of contract. |
| 8. | Amount of Bid Security to be Deposited | Rs. 50,000/-; in the form of Pay Order/ Call Deposit in favor of NEPRA.<br>The bid security will be released/returned for non-qualified firms. |
| 9. | Amount of Performance Security | 10% of the quoted amount in response of call off order. |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

# Table of Contents


1. INTRODUCTION: ..... 5
2. OBJECTIVE: ..... 5
3. SCOPE OF WORK: ..... 5
4. ELIGIBLE BIDDERS: ..... 8
5. ELIGIBILITY CRITERIA: ..... 8
6. INSTRUCTIONS TO SUBMIT THE PROPOSAL (PRE-QUALIFICATION DOCUMENT-PQD) ..... 8

F/A ..... 9

F/B ..... 11

F/C ..... 12

F/D ..... 13

F/E ..... 14

Annex-A ..... 15

Annex-B ..... 16


NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

## 1. INTRODUCTION:

National Electric Power Regulatory Authority (NEPRA), has been established as an independent Regulatory Authority under section 3 of Generation, Transmission and Distribution of Electric Power, Act 1997 for regulating the provision of electric power sector in Pakistan.

This Pre-Qualification Document (PQD) enlists the criteria for Cyber security firms/service Providers interested in engaging with NEPRA through Open Framework Agreement(s). Bidders are required to provide information as mentioned in clause No.7 of these documents.

## 2. OBJECTIVE:

NEPRA is seeking proposals from qualified cyber security firms/service providers to enhance the cyber security posture of existing ICT Infrastructure, support and implementation of robust cyber security measures for new ICT Infrastructure and cyber security related trainings.

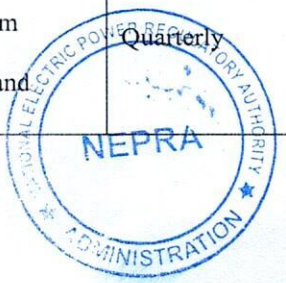
## 3. SCOPE OF WORK:

The selected firm is expected to provide following cyber security services and solutions at NEPRA premises:

| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| **Cybersecurity Services for ICT Infrastructure & Applications** | | |
| Vulnerability and Risk Assessments | • Comprehensive assessment report<br>• Prioritized list of vulnerabilities and associated risks<br>• Remediation recommendations and risk mitigation strategies | • Existing ICT Infrastructure: Annually<br>• For New Applications: As needed, based on new developments<br>• For Exisitng Applications: On changes or updates to the applications. |
| Secure Network Architecture | • Proposed/revised architecture diagram<br>• Documentation of security controls within the network<br>• Implementation plans for defense in depth<br>• Network segmentation plans and diagrams<br>• Secure Configuration baselines for network devices | Once |
| SLAs Review and Recommendations | • Assess existing hosting service contracts to incorporate robust cybersecurity clauses.<br>• Recommend improvements to clarify cybersecurity responsibilities and obligations between parties | Once |
| Outsourced Services Cybersecurity Assessment: | • Conduct a comprehensive cybersecurity assessment of outsourced services and third-party vendors.<br>• Identify potential vulnerabilities and risks, and establish protocols for risk mitigation and management. | yearly and on changes or updates |
| Operating System Hardening and CIS Benchmark Review | • Perform rigorous OS hardening procedures on existing servers to minimize attack vectors.<br>• Review and enhance configurations based on industry-standard benchmarks such as CIS to fortify defenses against zero-day attacks and APT threats. | Once |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| WAF Configuration/Firewall Evaluation | • Review Web Application Firewall (WAF) configurations to ensure optimal protection against web-based threats.<br>• Analyze rule sets and policies for effectiveness in mitigating common and emerging web application vulnerabilities. | yearly |
| Endpoint Security Solutions | • Review endpoint security solution<br>• Reports on endpoint protection status<br>• Vulnerability scanning on endpoints | yearly |
| Security Policies and Procedures | • Development of comprehensive security policies covering at least the following areas:<br>- Access Control Policy<br>- Network Security Policy<br>- Internet and email usage policy<br>- Acceptable use policy<br>- Information Security policy<br>- Data backup and recovery policy<br>- Data protection policy<br>- Social media usage policy<br>- Network Monitoring policy etc.<br>• Review of existing policy | Once |
| Incident Response Plan | • Documented incident response plan<br>• Roles and responsibilities involved in incident response<br>• Incident classification and prioritization criteria<br>• Communication protocols during incidents | Once |
| Disaster Recovery Planning and Procedures | • Detailed recovery plan and procedure<br>• Contact lists and communication plans<br>• Recovery time objectives (RTO) and recovery point objectives (RPO) | Once |
| Cybersecurity Requirements and Frameworks | • Prioritized list of cybersecurity requirements based on organizational needs.<br>• Framework documentation aligned with industry standards such as NIST Cybersecurity Framework or CIS Controls. | Once |
| Automated Backup Solutions | • Implementing automated backup processes to ensure regular and consistent data backups without manual intervention.<br>• Customizable backup schedules based on your organization's needs and operational requirements. | Once |
| Cybersecurity Threat Intelligence Feed | • Regular updates on emerging threats and vulnerabilities relevant to the organization.<br>• Analysis reports on the potential impact of threats on existing infrastructure. | Continuous |
| Incident Response Services and Forensics Services | • Incident response support and services for different types of cybersecurity incidents.<br>• Forensic analysis reports providing insights into the root cause of security incidents. | As needed based on incidents |
| Cybersecurity Management Support | | |
| Security Patching | • Updating and patching security systems to address vulnerabilities<br>• Evaluation reports on the impact of patches on system performance and functionality.<br>• Trend analysis reports highlighting patching trends and effectiveness over time. | Quarterly |



| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| Disaster Recovery Testing | • Detailed documentation of test scenarios and methodologies used.<br>• Post-testing evaluation reports including lessons learned and recommendations for improvement.<br>• Updated disaster recovery plans incorporating findings from testing exercises. | Annually |
| Compliance Audits | • Documentation of audit findings and observations.<br>• Remediation progress reports tracking the implementation of corrective actions.<br>• Regular communication with stakeholders on compliance status and areas needing improvement. | Annually |
| **Additional Related Work** | | |
| Software for Cybersecurity Compliance and Incident Reporting Portal, Power CERT portal | • Develop and implement cybersecurity compliance software.<br>• Incident reporting portal<br>• Power CERT portal for real-time threat intelligence sharing and collaboration. | Once |
| Development of Data Governance Framework | • Documented data governance policies and procedures.<br>• Data classification guidelines and implementation plan.<br>• Training materials for employees on data governance best practices. | Once |
| Implementation of ITIL Framework | • Implemented ITIL framework tailored to the organization's needs.<br>• Service catalog documenting IT services and their associated processes.<br>• Incident management procedures aligned with ITIL guidelines. | Annually |
| **Advanced Cybersecurity Solutions Implementation** | | |
| Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) | • Implemented IDS/IPS solutions with configuration documentation<br>• Regular reports on detected threats and prevented incidents<br>• Tuning and optimization reports for effectiveness | Once |
| Security Operations Center (SOC) | • Established and operational SOC with SOPs<br>• Documentation on SOC infrastructure and tools<br>• Incident response metrics and reports | Once |
| Security Information and Event Management (SIEM) | • Implemented SIEM solution with integration documentation<br>• User training materials for SIEM usage<br>• Regular reports on security events and incidents | Once |
| Security Orchestration, Automation, and Response (SOAR) | • Implemented SOAR platform<br>• Training for SOAR usage<br>• Assessment reports on automated response effectiveness | Once |
| **ISMS ISO 27001 Compliance Preparation** | | |
| Information Security Management System (ISMS) | • Developed, implement, and maintain ISMS alignment with ISO 27001 standards.<br>• Guiding NEPRA through necessary processes and procedures ensuring alignment with international best practices such as ISO 27001 and industry standards. | Once |
| Any Other Cybersecurity Related Work after Approval of the NEPRA Authority | | As needed |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

## 4. ELIGIBLE BIDDERS:

Only those companies and firms who have valid Income Tax and Sales.

## 5. ELIGIBILITY CRITERIA:

### 5.1 MANDATORY MINIMUM BASELINE CRITERIA FOR FIRMS/ COMPANIES/ BIDDERS

| Sr. No | Parameter | YES | No |
|---|---|---|---|
| 1. | Active Tax Payer + Sales tax registration | | |
| 2. | Registration with SECP | | |
| 3. | Six (06) years of Incorporation Time | | |
| 4. | Cyber security related experience (At least five (05) Cyber Security Audits/ Pen-testing/ Red Teaming Projects/ISMS ISO 27001 Implementation) | | |
| 5. | Firm should not be blacklisted in the public/private sector in Pakistan or abroad | | |
| 6. | Minimum ten (10) no. of Cyber security Professionals | | |
| 7. | Minimum seven (07) no. of Certified Cyber security Professionals<br>o Qualifying Certification Bodies (ISACA, (ISC)2, EC-Council, Offensive Security, SANS, ISO, ISA IEC 62443 Certification) | | |

**Note:**

a. Proof of aforesaid parameters must be provided.
b. Outsourcing of cyber security services to local/foreign 3rd parties is not allowed.
c. The proposals of Bidders, who fail to provide supporting documents will not be considered for pre-qualification.

## 6. INSTRUCTIONS TO SUBMIT THE PROPOSAL (PRE-QUALIFICATION DOCUMENT-PQD)

The bidders are directed to complete the following forms and submit with signature and seal on every page:

| Sr. No | Forms | Page# | Flags |
|---|---|---|---|
| 1 | UNDERTAKING | 9-10 | F/A |
| 2 | BASIC INFORMATION OF APPLICANT | 11 | F/B |
| 3 | PARTICULARS OF CYBER SECURITY RESOURCES | 12 | F/C |
| 4 | AFFIDAVIT FOR NON-BLACKLISTING OF FIRM | 13 | F/D |
| 5 | CONFLICT OF INTEREST | 14 | F/E |

**Briefly explain Firm/Company Business Details (Solutions and Services Offered):**

Name of the Bidder: _____

**UNDERTAKING:**

That the information submitted in the Pre-Qualification Documents is true; whereby, found false or deceptive, NEPRA reserves the right to disqualify the bidder from existing and all of the future biddings as per PPRA Rules.

**Seal and Signature of the bidder with date:**

---

**General Terms and Conditions**

1. Bid Security amounting to Rs. 50,000/- (refundable) in the form of Pay Order/ Call Deposit in favour of NEPRA must be attached with the submitted bid(s). No bid will be accepted without the bid security.
2. The bid security will be released/returned for non-qualified firms/bidders.
3. Successful bidder(s) will submit 10% of the quoted amount in response of call off order as Performance Security Deposit along with the contract agreement, which will be released only upon successful completion of the contract period (i.e. three years).
4. Cyber security related services and solutions through Open Framework Agreement shall be made by the successful bidder(s) at NEPRA Tower without any extra/additional charges with the issuance of call off order /work order.
5. Cyber Security Firm/ Service Provider should be registered with SECP or relevant Registrar of firms. Company/firm should appear Active Taxpayer list (ATL) of income and sales tax issued by FBR. The bidder(s) must attach substantial evidence with the bid regarding their registrations, experience and an affidavit that the firm has not been blacklisted by any Government/Semi Government organization.
6. Cyber Security firm/ service provider should not outsource its Cyber security related services to any local/foreign 3rd party.
7. Foreign companies having their local representation Branch office in Pakistan can also apply, subject to registration with SECP and FBR or relevant registrar of firms in Pakistan.
8. Cyber Security firm/ service provider should not be a blacklisted firm/company in Public/Private sector within Pakistan or abroad, due to any factor including but not limited to unsatisfactory performance, breach of general/specific instructions or NDA, corrupt practices and/or any fraudulent activity.
9. Cyber security audit firm should have documented policies and procedures including but not limited to Information Security processes and procedures, Personnel security and development.
10. While assessing the cyber security firm/ service provider, NEPRA may review several key areas of discipline including but not limited to profiles of certified individuals/resources, policies, Information sharing policy and procedure, Tools and reporting methodology.

NEPRA ADMINISTRATION

11. List of approved Cyber security Firms/ Service Providers will be published on NEPRA website and will be updated on regular basis.
12. Upon being listed under Cyber Security firms/ service providers approved list, NEPRA reserves the right to conduct a full assessment at any given point of time, which may require re-submission of all relevant documents submitted at the time of pre-qualification or any other additional document which may be required for additional scrutiny.
13. In case of violation of any clause in the Non-Disclosure Agreement (NDA), the approved Cyber Security firm/ service provider, is mandated to provide information including necessary details to NEPRA. In that case, NEPRA reserves the right to remove its name from pre-qualified Cyber Security firm/ service provider list and initiate legal proceedings wherever necessary.
14. NEPRA reserves the right to revise Cyber Security Firm/ Service Provider Pre-Qualification Criteria at any given point of time on need basis. approved Cyber security Firms/ Service Providers shall be apprised prior to revision of this criteria.
15. NEPRA shall evaluate the Prequalification Proposals in a manner prescribed in advance and may reject any Proposal which doesn't conform to the specified requirements.
16. For each call off order, NEPRA shall call up quotations in sealed envelope as Annexed (**A**) to this document from the pre-qualified firms/ service providers on its panel and award the work to the firm/service provider who quoted the lowest rates; however, if two or more pre-qualified firms/ service providers quote same rates for either of the job assignments, **the bidder/firm/service provider who may provide the required services in the shortest possible time, will be given preference**.
17. After the pre-qualification, the shortlisted firms/ service providers will have to sign the agreements within 7 days after intimation by NEPRA; otherwise, will be debarred from the right of placement on NEPRA's panel.
18. Payment to the selected firms/ service providers will be made by NEPRA within two weeks on production of the following subject to deduction of all taxes as per government law:
    (a) Bill(s) in original
    (b) Delivery Challan(s)
    (c) NEPRA Work Order(s)
    (d) Work Completion Certificate
19. The bidder himself will be responsible for ensuring that the EOI submitted is in accordance with the instructions stated herein. Any EOIs not submitted within the prescribed deadline will not be considered / entertained.
20. The bidder cannot modify or withdraw his bid after submission.
21. NEPRA reserves the right to forfeit the performance security deposit in case of breach of any clause of the contract by the contractor.
22. Sealed PQD along-with required documents must be delivered to this office by 6th day of May, 2024 before 1400 hrs and will be opened the same day at 1430 hrs in the presence of available participants.
23. NEPRA may on need basis pre-qualify new firms/ service providers during continuity of framework agreements in terms of Regulation 16(A)(5) of PPRA Rules, with previously pre- qualified firms/ service providers.
24. NEPRA reserves the right to accept or reject all bids as per PPRA rules.
25. Bidders are also required to submit the details on the prescribed proforma attached herewith the tender documents for correspondence. Moreover, the bidders are also required to provide complete profile, details if required.

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

## BASIC INFORMATION OF APPLICANT

**Prospective Applicant**

(a) Name:_____

(b) Address of the corporate headquarters and its branch office (s), Pakistan: _____

(c) Branches/Sub-offices/Subsidiaries Overseas (if any): _____

(d) Date of incorporation and / or commencement of business:_____

(e) Type (corporation, partnership, etc):_____

(f) Telephone No:_____

(g) Cell No:_____

(h) Fax:_____

(i) Email:_____

(j) NTN Registration No._____ and STN _____

(k) Registration with SECP:_____

(l) Registration with professional body:_____

**Details of individual (s) who will serve as the point of contact / Communication for the Bidder's company:**

(a) Name:_____

(b) Designation:_____

(c) Address:_____

(d) Telephone No._____

(e) Cell No. _____

(f) E-mail address:_____

(g) Fax No._____

Signature & Seal of Authorized Representative

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

F/C

**Particulars of Cyber security resources**

| S. No | Name of Individual | CNIC/Passport No | Cyber Security Experience (In Years) | Pentesting / Red teaming Experience (In Years) | Experience Details (organization names and duration only) / LinkedIn profile (if any) | Certifications Details (Expiry Date (if any), certification No.) |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | | | | | | |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

Affidavit for Non-Blacklisting of Firm
***[PRINT ON STAMP PAPER]***

Non-judicial stamp paper (with a value of Rs. 100) Date: _____

## AFFIDAVIT

It is hereby solemnly confirmed and declared that M/s ---------- , is declaring on oath that the Applicant:

- is not in *bankruptcy* or liquidation proceedings;
- has *never* been declared *ineligible/blacklisted* by Government / Semi-Government / Agency or Authority or any employer till date due to the any reasons
- is not making any *misrepresentations* or concealing any material fact and detail;
- has not been convicted of, fraud, *corruption*, collusion or money laundering;
- is not aware of any conflict of interest or potential *conflict of interest* arising from prior or existing contracts or relationships which could materially affect its capability to comply with its obligations; and
- does not fall within any of the circumstances for *ineligibility* or disqualifications

(Stamp of Company)
(Signatures of Authorized Rep)

_____
Company Name

**Attestation by Oath Commissioner and/or Notary Public**

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

# *CONFLICT OF INTEREST*

***Undertaking***

I hereby certify that to my knowledge, there is no conflict of interest involving the vendor named below:

*i.* No NEPRA official or employee has an ownership interest in vendor's company or is deriving personal financial gain from this contract.

*ii.* No NEPRA official's or employee's immediate family member has an ownership interest in vendor's company or is deriving personal financial gain from this contract.

*iii.* No retired or separated NEPRA official or employee, who has been retired or separated from the organization for less than two (2) years has an ownership interest in vendor's company.

*iv.* No NEPRA official or employee is contemporaneously employed or prospectively to be employed with the vendor.

*v.* Vendor hereby declares it has not and will not provide gifts or hospitality of any rupee value or any other tokens to any NEPRA official or employee to obtain or maintain a contract.

*vi.* Please note any exceptions below:

a. Vendor Name: _____

b. Vendor Phone No: _____

c. Conflict of Interest Disclosure:

i. Name and designation of NEPRA Official, employee or immediate family members with whom there may be a potential conflict of interest: _____

ii. Relationship to official: _____

iii. Interest in vendor's company: _____

iv. Any Other Information: _____

4. I certify that the information provided is true and correct by my signature below:

Name & Signature of Vendor: _____

Date: _____

CNIC /NTN No: _____

**Witness Information**:

1. Name: _____

2. CNIC No.: _____

3. Name: _____

4. CNIC No.: _____

**Annex-A**

## CALL OFF ORDER / CALL UP QUOTATIONS

To,
ABC, Resident Off,
Islamabad/Rawalpindi.
Tel:

Subject: **CALL OFF QUOTATION FOR CYBER SECURITY SERVICES/SOLUTIONS**

In pursuance of Pre-Qualification Document No._/2024 and the Open Framework Contract Agreement between NEPRA and your Company/Firm, the call off order is placed for providing the following cyber security services/solutions in terms of relevant provisions of the pre-qualification documents and contract agreement:

| Sr. No. | Description | Unit Price without GST | GST | Total Price inclusive of Tax |
|---|---|---|---|---|
| 1. | Work related to Cyber security as per scope | | | |
| | | | Total Price without Tax | |
| | | | Total GST | |
| | | | Total Price Inclusive of Taxes | |

2. You are required to fill in the table above and submit rates within seven (07) days of issuance of this call off order at the office of Director General (Admin./HR), NEPRA Tower Attaturk Avenue (East), G-5/1, Islamabad in a sealed envelope.

3. Non-Disclosure Agreement NDA will be signed after award of the work

Director (Administration)

**Submission:**

I hereby take on to provide the above-mentioned services within___number of days after receipt of the work order from NEPRA.

Seal of Bidder
(Name of Bidder)
Date:_____

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

**Annex-B**

## Contract Agreement

### Provision of Cyber Security Services & Solutions at NEPRA Tower

THIS AGREEMENT for Provision of Cyber Security Services & Solutions at NEPRA Tower (Hereinafter called the "Agreement) is made on____day of____2024.

**Between**

**National Electric Power Regulatory Authority (NEPRA)** (hereinafter referred to as the "Client", which expression shall, where the context so permits, be deemed to include its successor-in-interest and permitted assigns) of the one part;

**And**

M/s _____ (hereinafter referred to as the "Contractor") of the other part;
(The Client and Contractor shall, hereinafter collectively be referred to as the "parties" and individually as the "party")

**Recitals**

i) Whereas, the Contractor has shown its intention to provide cyber security services and solutions at NEPRA Tower, Attaturk Avenue (East) G-5/1, Islamabad;

ii) Whereas, the Client is desirous to hire the services of the Contractor and the Contractor has agreed to provide the same to the Client in consideration of the agreed payments to be made by the Client to the Contractor;

NOW THEREFORE, for good and valuable consideration, the receipt and sufficiency of which hereby acknowledged, the Parties agree and covenant as follows:

**Scope of Work**

The contractor agrees for the provision of the cyber security services and solutions at the NEPRA Tower Islamabad, at the following locations on 12 hours shift basis:

| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| **Cybersecurity Services for ICT Infrastructure & Applications** | | |
| Vulnerability and Risk Assessments | • Comprehensive assessment report<br>• Prioritized list of vulnerabilities and associated risks<br>• Remediation recommendations and risk mitigation strategies | • Existing ICT Infrastructure: Annually<br>• For New Applications: As needed, based on new developments<br>• For Exisitng Applications: On changes or updates to the applications. |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| Secure Network Architecture | • Proposed/revised architecture diagram<br>• Documentation of security controls within the network<br>• Implementation plans for defense in depth<br>• Network segmentation plans and diagrams<br>• Secure Configuration baselines for network devices | Once |
| SLAs Review and Recommendations | • Assess existing hosting service contracts to incorporate robust cybersecurity clauses.<br>• Recommend improvements to clarify cybersecurity responsibilities and obligations between parties | Once |
| Outsourced Services Cybersecurity Assessment: | • Conduct a comprehensive cybersecurity assessment of outsourced services and third-party vendors.<br>• Identify potential vulnerabilities and risks, and establish protocols for risk mitigation and management. | yearly and on changes or updates |
| Operating System Hardening and CIS Benchmark Review | • Perform rigorous OS hardening procedures on existing servers to minimize attack vectors.<br>• Review and enhance configurations based on industry-standard benchmarks such as CIS to fortify defenses against zero-day attacks and APT threats. | Once |
| WAF Configuration/Firewall Evaluation | • Review Web Application Firewall (WAF) configurations to ensure optimal protection against web-based threats.<br>• Analyze rule sets and policies for effectiveness in mitigating common and emerging web application vulnerabilities. | yearly |
| Endpoint Security Solutions | • Review endpoint security solution<br>• Reports on endpoint protection status<br>• Vulnerability scanning on endpoints | yearly |
| Security Policies and Procedures | • Development of comprehensive security policies covering at least the following areas:<br>- Access Control Policy<br>- Network Security Policy<br>- Internet and email usage policy<br>- Acceptable use policy<br>- Information Security policy<br>- Data backup and recovery policy<br>- Data protection policy<br>- Social media usage policy<br>- Network Monitoring policy etc.<br>• Review of existing policy | Once |
| Incident Response Plan | • Documented incident response plan<br>• Roles and responsibilities involved in incident response<br>• Incident classification and prioritization criteria<br>• Communication protocols during incidents | Once |
| Disaster Recovery Planning and Procedures | • Detailed recovery plan and procedure<br>• Contact lists and communication plans<br>• Recovery time objectives (RTO) and recovery point objectives (RPO) | Once |
| Cybersecurity Requirements and Frameworks | • Prioritized list of cybersecurity requirements based on organizational needs.<br>• Framework documentation aligned with industry standards such as NIST Cybersecurity Framework or CIS Controls. | Once |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| Automated Backup Solutions | • Implementing automated backup processes to ensure regular and consistent data backups without manual intervention.<br>• Customizable backup schedules based on your organization's needs and operational requirements. | Once |
| Cybersecurity Threat Intelligence Feed | • Regular updates on emerging threats and vulnerabilities relevant to the organization.<br>• Analysis reports on the potential impact of threats on existing infrastructure. | Continuous |
| Incident Response Services and Forensics Services | • Incident response support and services for different types of cybersecurity incidents.<br>• Forensic analysis reports providing insights into the root cause of security incidents. | As needed based on incidents |
| **Cybersecurity Management Support** | | |
| Security Patching | • Updating and patching security systems to address vulnerabilities<br>• Evaluation reports on the impact of patches on system performance and functionality.<br>• Trend analysis reports highlighting patching trends and effectiveness over time. | Quarterly |
| Disaster Recovery Testing | • Detailed documentation of test scenarios and methodologies used.<br>• Post-testing evaluation reports including lessons learned and recommendations for improvement.<br>• Updated disaster recovery plans incorporating findings from testing exercises. | Annually |
| Compliance Audits | • Documentation of audit findings and observations.<br>• Remediation progress reports tracking the implementation of corrective actions.<br>• Regular communication with stakeholders on compliance status and areas needing improvement. | Annually |
| **Additional Related Work** | | |
| Software for Cybersecurity Compliance and Incident Reporting Portal, Power CERT portal | • Develop and implement cybersecurity compliance software.<br>• Incident reporting portal<br>• Power CERT portal for real-time threat intelligence sharing and collaboration. | Once |
| Development of Data Governance Framework | • Documented data governance policies and procedures.<br>• Data classification guidelines and implementation plan.<br>• Training materials for employees on data governance best practices. | Once |
| Implementation of ITIL Framework | • Implemented ITIL framework tailored to the organization's needs.<br>• Service catalog documenting IT services and their associated processes.<br>• Incident management procedures aligned with ITIL guidelines. | Annually |
| **Advanced Cybersecurity Solutions Implementation** | | |

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY
NEPRA
ADMINISTRATION

| Service Description | Anticipated Deliverables | Frequency |
|---|---|---|
| Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) | • Implemented IDS/IPS solutions with configuration documentation<br>• Regular reports on detected threats and prevented incidents<br>• Tuning and optimization reports for effectiveness | Once |
| Security Operations Center (SOC) | • Established and operational SOC with SOPs<br>• Documentation on SOC infrastructure and tools<br>• Incident response metrics and reports | Once |
| Security Information and Event Management (SIEM) | • Implemented SIEM solution with integration documentation<br>• User training materials for SIEM usage<br>• Regular reports on security events and incidents | Once |
| Security Orchestration, Automation, and Response (SOAR) | • Implemented SOAR platform<br>• Training for SOAR usage<br>• Assessment reports on automated response effectiveness | Once |
| ISMS ISO 27001 Compliance Preparation | | |
| Information Security Management System (ISMS) | • Developed, implement, and maintain ISMS alignment with ISO 27001 standards.<br>• Guiding NEPRA through necessary processes and procedures ensuring alignment with international best practices such as ISO 27001 and industry standards. | Once |
| Any Other Cybersecurity Related Work after Approval of the NEPRA Authority | | As needed |

## SECTION-2

## General Terms and Conditions

1. The Contractor shall not transfer, assign, pledge or subcontract the assigned job to any other firm.
2. Taxes would levy as per the rules of the Government. The Contractor cannot modify or withdraw his offered rates after submission of invoice.
3. The Client shall make payment to the Contractor as per actual after successful completion of work.
4. In case of any dispute or difference, the case will be settled amicably between both the parties.
5. In the event of failure of amicable settlement of dispute as above, either party of this contract may refer the matter of dispute to arbitration under the provision of Arbitration Act, 1940 and the rules issued thereunder, at Islamabad, Pakistan.
6. The Client can include/exclude terms and conditions if required.
7. The terms & conditions mentioned in the pre-qualification document shall be the part and parcel of this agreement.
8. After the successful award of the work, a Non-Disclosure Agreement (NDA) will be executed. This legal contract is designed to safeguard confidential information exchanged during the course of the project, ensuring that both parties can collaborate securely, protecting proprietary details, and maintaining the integrity of sensitive data throughout our engagement

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION

**Section – 3**

**CURRENCY OF AGREEMENT**

The Agreement shall come into force immediately upon signing by both parties and shall remain valid for three years.

**IN WITNESS WHEREOF**, THE PARTIES HAVE HEREUNDER SET THEIR HANDS ON THE DAY AND THE YEAR FIRST WRITTEN ABOVE.

| **For and on behalf of the Client (NEPRA)** | **For and on behalf of Contractor M/s** |
|---|---|
| _____ | _____ |
| Director (Administration) | (_____) CEO |

**1. WITNESS**

Name: _____

CNIC No. _____

**2. WITNESS**

Name: _____

CNIC No. _____

NATIONAL ELECTRIC POWER REGULATORY AUTHORITY NEPRA ADMINISTRATION