**الملحق )أ( نطاق الأعمال**

**Annex A Scope of Work**



**نطاق الأعمال**

**Scope of Work**

### INTRODUCTION

The Ministry of Public Health (MOPH) Information department hereby invites interested competitive bidders to tender for Vulnerability Assessment and Penetration Testing (VAPT) Services to cover the below technical requirements with continuous support on performing the VAPT cycles for the period of three (3) years.

### THE OBJECTIVE:

This is to establish a partnership with a qualified cybersecurity service provider to deliver an integrated, adaptive security validation and resilience framework across our enterprise IT, Cloud environments.

This initiative aims to move beyond traditional point-in-time security assessments by implementing a Penetration Testing program covering external and internal networks, cloud infrastructures, Kubernetes environments, wireless systems, VoIP technologies, Source code and application layers — ensuring ongoing identification and validation of vulnerabilities as the threat landscape evolves.

In parallel, the engagement seeks to deploy and integrate a centralized Risk Operation Center platform to consolidate vulnerability data, risk prioritization, penetration testing activities, remediation tracking, and compliance reporting. This platform must support real-time integration with existing vulnerability scanners, asset inventories, and ticketing systems to enable a single pane of glass for enterprise risk management.

The end goal is to ensure that security validation becomes an ongoing operational process rather than a periodic event, while simultaneously building MOPH resilience against advanced cyber threats through proactive detection, rapid response, risk-driven remediation, and continuous improvement mechanisms.

The selected partner must demonstrate a proven capability to deliver these services with measurable outcomes aligned to risk reduction, compliance mandates, and business continuity objectives.

### SCOPE OF WORK:

##### Deliverable

* + 1. **Executive Summary Report**

High-level overview of key findings, business risks/impact, Risk Posture rating and strategic recommendations for management.

##### Technical Findings Report

A detailed report of all discovered vulnerabilities and misconfigurations, including but not limited to descriptions, risk severity ratings (e.g., CVSS), proof of concept with supporting evidence, affected systems, relevant screenshots or logs, and categorization based on industry standards such as OWASP Top 10 and CWE.



##### Objective-Based Attack Scenarios

Provide detailed documentation of penetration testing activities aligned with defined objectives, including but not limited to authentication bypass, data exposure, misconfigurations, injection attacks, privilege escalation, and data exfiltration. Include descriptions of all attempted attack paths, methodologies, and outcomes, mapping each to its test objective to assess security posture and impact.

##### Remediation Recommendations

Provide clear and actionable guidance for each finding, including but not limited to a prioritized remediation plan categorized into short-, medium-, and long-term actions, supported by references to best practices, vendor patches, and configuration guidelines. Etc.

* + 1. **Dashboard and Portal access to manage the platform**
    2. **Integration with risk management platform within 3 months.**
    3. **Training and knowledge transfer sessions for team members.**
    4. **Cleanup Report with Evidence**
    5. **Any exploit which can impact the functionality or business operation interruption needs to be informed and discussed first**
    6. **Retesting Report (if applicable)**
       1. Summary of vulnerabilities retested
       2. Updated status (resolved, still vulnerable, etc.)
       3. Verification evidence
       4. The vendor should be prepared to accommodate additional requirements that emerge during the course of the project, based on situational demands

##### Key Performance Indicators (KPIs)

To ensure transparency, accountability, and measurable success, the following KPIs will be used to evaluate vendor performance and project outcomes:

##### Coverage & Scope

* + - * + % of assets tested (networks, cloud, applications, etc.)
        + Scope adherence rate (coverage of agreed environments)

##### Vulnerability Identification

* + - * + Number of vulnerabilities discovered (by severity)
        + False positive rate
        + Exploit success rate

##### Revalidation testing

* + - * + Retest success rate of remediated findings



##### Reporting & Documentation

* + - * + Timeliness of report delivery (draft and final)
        + Quality of executive summaries and technical findings
        + Format compatibility with internal systems

##### Risk Operations Center platform Integration

* + - * + % of tools successfully integrated (Vulnerability scanners, inventories, ticketing)
        + Real-time data sync success rate
        + Dashboard uptime and availability

##### Compliance & Standards

* + - * + Alignment with QCSF, NIA,CIS, OWASP, NIST, ISO 27001, etc.
        + % of compliance gaps identified and addressed

##### Operational Efficiency

* + - * + Milestone achievement rate
        + Change request handling time
        + Stakeholder communication responsiveness

##### Security Posture Improvement

* + - * + Risk score reduction post-remediation
        + Continuous improvement recommendations implemented

##### L-External Network Map

Diagram or summary of the External topology and lateral movement paths identified during the assessment.

#### Detailed Scope of Work

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
| **1** | **External Penetration Testing** | 700 Public Ips | black-box testing of all internet-facing  services to identify exploitable  vulnerabilities and weak configurations (not limited to) using objective-based  penetration testing | - Reports and attack of all exploitable vulnerabilities and  misconfigurations including  remediation steps | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  | methods. , website  scraping, defacement | * Dashboard and Portal access to manage the platform * Integration with risk management platform. * Training and knowledge   transfer sessions for team  members. |  |
| **2** | **Internal Penetration Testing** | 3000 Internal IPs including: - Active  Directory - Azure AD - Microsoft Exchange / O365 -  IIS/Apache - SQL, ERP, File  Services - NAC/Endpoint Security Bypass  - IAM/PAM  but not limited to | internal testing to identify lateral movement paths, privilege escalation, domain takeover  scenarios, and internal  misconfigurations, clean up etc but not limited to | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * Dashboard and Portal access to manage the platform * Integration with risk management platform within 3 months. | - Every Year once – upto 3 Years |
| **3** | **Wi-Fi Security Testing** | 7 SSIDs (Head Office) | Evaluate Wi-Fi  security controls, encryption, rogue access points, and  unauthorized access attempts across the head office premises. | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the   vulnerability  tracking platform | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  |  |  |  |
| **4** | **External Web**  **Application Security Assessment** | 100 External Web Apps | Manual and automated testing of external-facing  applications for OWASP Top 10 and business logic flaws. website scraping, defacement | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. | - Every Year once – upto 3 Years |
| **5** | **API Security Assessment** | Blackbox | * Find publicly exposed APIs and identify potential misconfiguration and loopholes. * In depth testing for business logic and access   control  vulnerabilities.   * OWASP Top 10   testing | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. | - Every Year once – upto 3 Years |
| **6** | **ERP Security Assessment** | 2 ERP  Applications | An in-depth security assessment targeting ERP systems to  evaluate | - Reports and attack of all exploitable  vulnerabilities | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  | authorization controls, and ERP-  specific security gaps, including but not  limited to user access management,  segregation of duties, and configuration weaknesses. The  assessment aims to identify  vulnerabilities that could impact the confidentiality, integrity, and  availability of critical business processes. | and  misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. |  |
| **7** | **Internal Web**  **Application Security Assessment** | 10 Internal Applications | Focused on internal portals, custom web apps, and services critical to internal operations. website  scraping, defacement | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. | - Every Year once – upto 3 Years |
| **8** | **Mobile Application Security Testing** | 3 Mobile Apps | Assessment of mobile apps (Android/iOS) including API calls, insecure storage,  reverse engineering, | - Reports and attack of all exploitable vulnerabilities and  misconfigurations | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  | and runtime manipulation. | including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. |  |
| **9** | **Configuration Review & System Hardening** | Sample of up to 100 IPs from: - Microsoft/Linux Servers - Databases -  Security/Netwo rk Devices -  SIEM/SOAR, AD  , azure cloud the list is not exhausted | Review of hardening benchmarks (e.g., CIS/NIST),  misconfigurations, and unnecessary  services across  servers and security infrastructure. | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. | - Every Year once – up to 3 Years |
| **10** | **VoIP Security Assessment** | 1 VoIP Network | Assessment of VoIP protocols (SIP/RTP), call spoofing,  eavesdropping, and unauthorized device registration. | * Reports and attack of all exploitable vulnerabilities and   misconfiguration s including  remediation steps   * On-boarding of   all vulnerabilities | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  |  | to the RM platform  Excel trackers for all vulnerabilities discovered with parsing support on RM platform. |  |
| **11** | **Advanced Social Engineering**  **Assessment** | 2000 Staff incl. Vendors technology vetting | Includes phishing, baiting, USB drops, and remote attack simulations,  especially targeting IT/application admins and privileged users. The assessment should be conducted to replicate a real  social engineering  assessment targeting MOPH users. No  whitelisting to be requested during the assessment. | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for all vulnerabilities discovered with parsing support on RM platform. | - Every Year once – upto 3 Years |
| **12** | **Source Code Review** | 10 Applications (max 1.5M LoC) | Static code analysis and manual review to identify logic flaws, insecure coding practices, and vulnerabilities.  Includes dev workshops for  remediation steps discussion. | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation steps insecure coding practices   * On-boarding of all vulnerabilities to the RM platform * Excel trackers for   all vulnerabilities | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  |  | discovered with parsing support on RM platform.  - SAST/DAST tool to be installed and used on MOPH  provisioned laptop |  |
| **13** | **Product Security Assurance Service** | Up to 2 Security  Products (EDR, Proxy, etc.) | Independently test security products against MITRE ATT&CK tactics to benchmark  prevention/detection capabilities without mixing with pentesting scope. | * Onboarding and access to the platform * Deployment of sensors across all endpoints * Training and knowledge   transfer sessions for team  members.   * Integration   support with RM platform. | - Every Year once – upto 3 Years |
| **14** | **Clean Up** | All | Clean up after all VAPT activities and stated in the completion report | * Reports and attack of all exploitable vulnerabilities and   misconfigurations including  remediation   * , clean steps and evidences | - Every Year once – upto 3 Years |
| **15** | **Risk Management Platform** | Hosted In- House  3000 Assets | Deploy a centralized Risk management platform for real-time tracking,  management, and prioritization of | * Identify all   external exposed APIs   * Identify loopholes and   misconfigurations  that can lead to | - Every Year once – upto 3 Years |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  | identified vulnerabilities.  Integrate with existing vulnerability scanners, asset management  systems, ticketing platforms, and threat intelligence feeds to create a unified risk management console.  Enable secure onboarding of  penetration testing activities, including project scoping, consultant  collaboration, task assignment, and  vulnerability lifecycle management.  Provide dashboards and reporting  features for risk visualization,  compliance tracking, SLA monitoring, and executive summaries.  Facilitate  collaboration  between internal teams and external  consultants through a secure portal, ensuring  transparency and  accountability | data exposure or breach confidentiality, integrity or  Availability. |  |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr. No.** | **Activity** | **In-Scope Items** | **Description** | **Deliverables** | **Frequency** |
|  |  |  | throughout  remediation efforts.  Risk Management Platform Certified against Qatar  Common Criteria  Scheme |  |  |
| **16** | **Detection and Response** | Hosted In- House | Red Team exercise for testing security monitoring solutions (e.g. SIEM) | - | - |

* 1. **Compliance Matrix Table**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**S.No**

**1**

**2**

**3**

**4**

**Section**

Vulnerability

Assessment and

Penetration Testing

Vulnerability

Assessment and

Penetration Testing

Vulnerability

Assessment and

Penetration Testing

Vulnerability

Assessment and

Penetration Testing

##### Sub-Section

Experience and Certifications

Experience and Certifications

Experience and Certifications

Experience and Certifications

##### Requirement

Consultants must have at least 5 years of relevant experience and shall be NCSA accredited security provider.

Required certifications: OSCE, OSCP, GPEN, CEH,

CISSP, CCIE, NIA, QCSF2022, ISO27001

Certified Professionals for Network Reviews and Configuration Audits Activities (CCIE, CISSP), 2 CCIE Certifications Resources Profiles along with QID need to be added in Proposal

The Project Manager assigned to this

engagement must be based in Qatar, possess a

minimum of 5 years of relevant project

management experience in cybersecurity or IT domains, and hold an

##### Compliance (Yes/No/Partial)

**Comments/Rem arks**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
|  |  |  | active PMP (Project  Management Professional) certification |  |  |
| **5** | Vulnerability  Assessment and  Penetration Testing | Experience and Certifications | The Bidder must  demonstrate proven expertise in advanced offensive security techniques, including but not limited to EDR/XDR  evasion, pRMess injection, DLP bypasses, advanced open-source intelligence  (OSINT) gathering, and red teaming tactics.  The proposal must include case studies or real-world examples showcasing successful execution of  these techniques in previous engagements. |  |  |
| **6** | Vulnerability  Assessment and  Penetration Testing | Experience and Certifications | The Bidder must include detailed methodologies and practical use cases  demonstrating customized exploitation techniques during application security assessments.  The Bidder must show the capability to develop and execute sophisticated  exploits, bypass established security controls, and  simulate advanced threat  scenarios to validate real- world risk exposures |  |  |
| **7** | Vulnerability  Assessment and  Penetration Testing | Experience and Certifications | Mention consultants'  certifications and provide QID copies in the technical proposal. (Minimum 5 Consultants QID should be submitted with the Proposal) |  |  |
| Page **43** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
| **8** | Vulnerability  Assessment and  Penetration Testing | Scope of Work and Methodology | Present a detailed scope of work, methodology, and  high-level plan with deliverables outlined before project award. |  |  |
| **9** | Vulnerability  Assessment and  Penetration Testing | Scope of Work and Methodology | The Bidder must  comprehensively cover all services, activities, and  deliverables outlined in the Scope of Work, ensuring full compliance with the technical, operational, and reporting requirements  defined in this RFP |  |  |
| **10** | Vulnerability  Assessment and  Penetration Testing | Scope of Work and Methodology | All tools, software,  appliances, and licenses required to perform the assessment, testing, and  analysis must be procured maintained, and fully borne by the Bidder without any additional cost to the  MOPH |  |  |
| **11** | Vulnerability  Assessment and  Penetration Testing | Scope of Work and Methodology | All services must be delivered on-premises within the MOPH’s  environment using locally available resources; no  remote delivery or offshore resources will be accepted for any phase of the  engagement |  |  |
| **12** | Vulnerability  Assessment and  Penetration Testing | Scope of Work and Methodology | The Bidder must initiate project activities within one  (1) week from the date of contract signing, ensuring timely mobilization of resources and kickoff of all planned deliverables  without delays |  |  |
| **13** | Vulnerability  Assessment and  Penetration Testing | Vulnerability Assessment and  Penetration Testing | Quality Assurance plan including Testing,  Validation, Acceptance Criteria |  |  |
| Page **44** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
| **14** | Vulnerability  Assessment and  Penetratio]n Testing | References | The Bidder must provide at least five (5) references for similar services successfully delivered within Qatar, including contact details  (name, designation, organization, email, and phone number) and a brief description outlining the project scope, key  deliverables, and achieved outcomes |  |  |
| **15** | Vulnerability  Assessment and  Penetration Testing | Reporting | The Bidder must submit  sample reports covering All Vulnerability Assessment and Penetration Testing  (VAPT), product security assurance services  The submitted reports must demonstrate the ability to effectively  identify, analyze, prioritize, and provide actionable  remediation guidance for security issues across  diverse environments |  |  |
| **16** | Risk Management Platform | Risk Management and Platform Capabilities | Vulnerability tracking, analysis, prioritization management |  |  |
| **17** | Risk Management Platform | Risk Management and Platform Capabilities | Manage penetration testing projects (internal, external, mobile, wireless, VOIP) |  |  |
| **18** | Risk Management Platform | Risk Management and Platform Capabilities | Dashboards for projects, findings, asset association |  |  |
| **19** | Risk Management Platform | Risk Management and Platform Capabilities | Integration with 3rd party tools (SIEM, SOAR, EDR/XDR) |  |  |
| **20** | Risk Management Platform | Risk Management and Platform Capabilities | Role-Based Access Control and MFA |  |  |
| **21** | Risk Management Platform | Risk Management and Platform Capabilities | Parsing Vulnerability Scanner Results |  |  |
| **22** | Risk Management Platform | Risk Management and Platform Capabilities | Findings status update and remediation tracking |  |  |
| Page **45** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
| **23** | Risk Management Platform | Risk Management and Platform Capabilities | Onboard External  Consultants with limited access |  |  |
| **24** | Risk Management Platform | Risk Management and Platform Capabilities | Customizable Report Templates |  |  |
| **25** | Risk Management Platform | Risk Management and Platform Capabilities | Integration with Ticketing Systems |  |  |
| **26** | Risk Management Platform | Risk Management and Platform Capabilities | On-Premises Deployment support |  |  |
| **27** | General Administrative Requirements | General Administrative Requirements | The Bidder must clearly disclose any subcontracting arrangements in the proposal.  If subcontractors are engaged, the Bidder  remains solely responsible for the complete delivery of services, quality,  timelines, and compliance with all RFP requirements |  |  |
| **28** | General Administrative Requirements | General Administrative Requirements | The Bidder must have a legally registered entity operating in Qatar for a  minimum of five (5) years prior to the date of this RFP submission. Proof of commercial registration and establishment must be  provided. |  |  |
| **29** | General Administrative Requirements | General Administrative Requirements | The Bidder shall not replace any resource  assigned to the project without prior written approval from the MOPH  after project initiation |  |  |
| **30** | General Administrative Requirements | General Administrative Requirements | The Bidder must maintain local operational and technical support  capabilities within Qatar for the entire duration of the project engagement and warranty period. |  |  |
| Page **46** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
| **31** | General Administrative Requirements | General Administrative Requirements | Statement of independence:  Bidders must testify for their independence considering the scope of work for the current project and previous  engagements with MOPH and that no conflict of interest exist if contract  awarded to them. |  |  |
| **32** | General Administrative Requirements | General Administrative Requirements | Bidder must provide financial statement for the last 3 years |  |  |
| **33** | General Administrative Requirements | General Administrative Requirements | Bidder must provide their ICV certificate |  |  |
| **34** | General Administrative Requirements | General Administrative Requirements | Bidder must provide  certificate of allocated resources has passed the security screening with no criminal records. |  |  |
| **35** | General Administrative Requirements | General Administrative Requirements | MOPH has right to audit the service provider as  applicable to the scope of work and/or request assurance reports provided through independent 3rd  parties |  |  |
| **36** | Risk Management Platform | Risk Management and Platform Capabilities | Services provided through the vendor that require obtaining access and authorization to the entity resources, should always be managed in a secure way (controlled and  monitored) in alignment with the entity Identify and Access Management policy and best practices (Least Privilege, Zero Trust, need  to know …etc.) |  |  |
| **37** | Change Management Platform | Change Management Requirements | Changes\Configs\Updates to in-scope solutions  /services should be planned, approved and  authorized in accordance to the “MOPH” relevant |  |  |
| Page **47** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
|  |  |  | policies (Change/Config Management) and best practices. |  |  |
| **38** | Risk Management Platform | Risk Management and Platform Capabilities | The service provider should follow rules of engagement as indicated by the NCSA and best practices such identifying sources/times of testing, prohibited  activities, approvals for  data dumps …etc. |  |  |
| **39** | Software solution requirements: | Software solution  requirements: | 1. Solution shall be certified against Common Criteria. 2. Solution shall be compliant with national   requirements (NIA, PDPPL  …etc.)   1. Security Baselines and hardening procedures should be established, documented and   implemented for the solution/technology   1. As-built documentation for the provided   solutions, architectural diagrams (Conceptual,  Logical, Physical) as needed   1. Secure access should be established to ensure proper implementation for identification,   authentication, authorization and  accountability such as MFA, RBAC, Security Monitoring  …etc.   1. Security monitoring will be supported and enabled for in scope solutions 2. Solutions will be free of vulnerabilities and updates/patches will be provided in timely manner with clear SLA 3. Tools, manuals and user   guides. etc. |  |  |
| Page **48** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | |
| **S.No** | **Section** | **Sub-Section** | **Requirement** | **Compliance (Yes/No/Partial)** | **Comments/Rem arks** |  |
|  |  |  | 9. Ownership Licenses and subscriptions for needed duration |  |  |
| **3.4 Project Management Requirements:**   1. **Understanding Project Scope and Objectives**    * **Requirement:** Clearly understand the scope of the VAPT engagement — systems, networks, applications, and infrastructure to be tested; exclusions; testing depth (e.g., black-box, white-box); and expected deliverables (e.g., detailed vulnerability reports, risk assessments, remediation guidance).    * **Importance:** Avoids ambiguity about what will be tested and aligns MOPH expectations, preventing scope creep and ensuring focused testing efforts. 2. **Detailed Project Planning and Scheduling**    * **Requirement:** Develop a timeline with key phases — reconnaissance, scanning, exploitation, reporting, and remediation verification. Include milestone deadlines, resource assignments (testers, toolsets), and integration points with MOPH operations (e.g., maintenance windows).    * **Importance:** Ensures smooth execution without disrupting MOPH operations and allows time for remediation and re-testing. 3. **Stakeholder Identification and Communication Management**    * **Requirement:** Identify all relevant stakeholders such as IT security teams, compliance officers, application owners, and management. Define communication plans for kick-off meetings, status updates, risk alerts, and delivery of final reports.    * **Importance:** Facilitates transparency, aligns expectations, and supports rapid response to findings or issues. 4. **Resource and Tool Management**    * **Requirement:** Assign experienced penetration testers with relevant certifications (e.g., OSCP, CEH) and ensure availability of approved tools (e.g., Nessus, Burp Suite, Metasploit). Manage access credentials and testing permissions securely.    * **Importance:** Guarantees that the team has the right expertise and tools, and operates within legal and ethical boundaries. 5. **Risk and Impact Assessment**    * **Requirement:** Identify potential risks such as unintended service disruption, data leakage, or false positives. Develop mitigation strategies, including testing during low-impact periods and having rollback plans.    * **Importance:** Protects MOPH operations and data integrity, maintaining trust and minimizing negative impact. 6. **Compliance and Legal Considerations**   Page **49** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | | |



* **Requirement:** Ensure all testing activities comply with applicable laws, regulations, and MOPH policies. Obtain formal written authorization before testing.
* **Importance:** Prevents legal issues and enforces ethical testing standards.

##### Change and Scope Management

* + **Requirement:** Define a process for handling scope changes, such as adding new systems or deeper testing. Changes must be approved by project sponsors and documented.
  + **Importance:** Controls project boundaries and resources, avoiding unplanned workload and budget overruns.

##### Quality Assurance and Validation

* + **Requirement:** Establish criteria for validating findings (e.g., verifying vulnerabilities with proof-of-concept) and review cycles for reports. Include peer reviews or audits of testing and documentation.
  + **Importance:** Ensures accuracy and credibility of the results, enhancing MOPH confidence.

##### Progress Monitoring and Status Reporting

* + **Requirement:** Use project management tools to track task completion, issue logs, and risk status. Provide regular updates to stakeholders, including interim findings if appropriate.
  + **Importance:** Enables timely detection of delays or blockers and facilitates stakeholder decision-making.

##### Incident Handling and Escalation Procedures

* + **Requirement:** Define processes for handling unexpected critical findings, security incidents during testing, or system outages caused by tests. Include clear escalation paths.
  + **Importance:** Ensures swift and coordinated responses to minimize damage and maintain MOPH trust.

##### Documentation and Knowledge Transfer

* + **Requirement:** Maintain detailed records of test plans, methodologies, tools used, findings, and remediation recommendations. Conduct final debrief sessions with MOPH teams.
  + **Importance:** Provides a comprehensive audit trail, supports remediation efforts, and helps build MOPH security maturity.

##### 3.5 Bill of Quantity:

|  |  |  |  |
| --- | --- | --- | --- |
| **SN** | **Product/Service Descriptions** | **UoM** | **Quantity** |
| **1** | Project Kick Off/Initiation | Lot | 1 |
| **2** | Year 1 scope, Vulnerability Assessment and Penetration Testing (VAPT), Documentation/Reports/Presentation/Revalidation | Lot | 1 |
| **3** | Year 2 scope, Vulnerability Assessment and Penetration Testing (VAPT), Documentation/Reports/Presentation/Revalidation | Lot | 1 |
| **4** | Year 3 scope, Vulnerability Assessment and Penetration Testing (VAPT), Documentation/Reports/Presentation/Revalidation | Lot | 1 |



**3.6 Compliance Matrix:**

Vendors should clarify on their proposal how MOPH requirements listed in the scope of work and technical evaluation criteria will be achieved by using a compliance check whose format is motioned below.

|  |  |  |  |
| --- | --- | --- | --- |
| **SN** | **Requirements** | **Compliance (Complied /**  **Not Complied)** | **Remarks** |
| 1.1 | Deliverable |  |  |
| 1.2 | **Detailed Scope of Work** |  |  |
| 1.3 | Compliance Matrix Table |  |  |
| 1.4 | Project Management Requirements |  |  |
| 1.5 | Bill of Quantity (BOQ) |  |  |
| 1.6 | Project Plan |  |  |
| 1.7 | Documentation and Knowledge Transfer |  |  |
| 1.8 | Delivery Terms |  |  |
| 1.9 | Licenses and Authority approvals |  |  |
| 1.10 | Risk Management Platform Certified against Qatar  Common Criteria Scheme |  |  |
| 1.11 | Service Level Agreement (SLA) |  |  |
| 1.12 | Non-Disclosure Agreement (NDA) |  |  |
| 1.13 | Contract Duration |  |  |
| 1.14 | Payment Method |  |  |

* Delivery to be completed **as per defined Milestones** from commencement date of the contract.

##### Project Plan (if applicable)

Upon commencement of the project, the bidder shall prepare a tool based, detailed project plan for the engagement. The plan should include detailed task and activities along with their dependencies, time and duration of each task and activity, deliverables, milestones, and resources allocation to each task and activity, assumptions, and constraints.

A sign-off from MOPH on the project plan shall be taken by the bidder. The approved project plan shall act as a baseline for the engagement. Project status for the entire engagement shall be measured based on the project plan prepared by the bidder.

##### Documentation and Knowledge Transfer

Vendors must provide the following.

* + 1. Proposal softcopy in searchable format.
    2. Project Plan in MS project
    3. Weekly project status report (MOPH will share the format)



* + 1. High-level Design documents if applicable.
    2. Standard operation procedure documents.
    3. Monthly Executive summary report.
    4. Technical Reports for the findings and Remediation Recommendations
    5. UAT / Signoff document for each milestone.
    6. Knowledge Transfer to MOPH staff.

##### Delivery Terms:

|  |  |  |
| --- | --- | --- |
| **Project**  **Milestones** | **Key Deliverables per Milestone** | **Date of**  **Completion** |
| **Milestone 1** | Project Kick Off | Q2 2026 |
| **Milestone 2** | Year 1 scope, VAPT, Documentation/Reports/Presentation/Revalidation | Q2 2027 |
| **Milestone 3** | Year 2 scope, VAPT, Documentation/Reports/Presentation/Revalidation | Q2 2028 |
| **Milestone 4** | Year 3 scope, VAPT, Documentation/Reports/Presentation/Revalidation | Q2 2029 |

* 1. **Licenses and authority approvals:**

No authority approval necessary.

##### Risk Management Platform Certified against Qatar Common Criteria Scheme:

The Risk Management Platform must be certified by Common Criteria Recognition Arrangement (CCRA) against Qatar Common Criteria Scheme Certification under National Cyber Governance and Assurance Affairs within National Cyber Security Agency (NCSA).

##### Service Level Agreement (SLA):

The Bidder shall adhere to the SLA as in **Appendix A.**

##### Non-Disclosure Agreement (NDA):

The Bidder shall adhere to the NDA as in **Appendix B.**



##### Contract Duration:

**3 Years** from the commencement date of the contract.

##### Payment method:

MOPH will verify the vendor’s performance of the deliverables outlined in the invoice before making payment.

The payment will be in Installments.

* 25% after Project initiation/completion of Milestone 1
* 25% after Delivery of service in first Year/completion of Milestone 2.
* 25% after Delivery of service in Second Year/completion of Milestone 3.
* 25% after Delivery of service in third year/completion of Milestone 4.

**Note:** Vendor to submit Quarterly health check report signoff from MOPH IS department along with the invoices for processing the end of 1st, 2nd and 3rd year payments.

##### Warranty and Maintenance.

Not Applicable

### EVALUATION CRITERIA:

Mandatory Evaluation Criteria are ‘must meet’ criteria. These criteria are assessed by MOPH’s evaluators on a Yes/No basis as to whether the criteria are met. The Mandatory Criteria will be evaluated based on the information provided in the bidder’s technical proposal. Bidders qualified with “Yes” in the mentioned mandatory criteria, in below Table 1, will qualify for technical evaluation.

|  |  |  |
| --- | --- | --- |
| **Sr.No** | **Mandatory Evaluation Criteria** | **YES/NO** |
| 1 | Bidder's experience and proven capability in implementing similar integrated projects in Enterprise Government & Semi-Government sector **for 5 years minimum**. ***(Evidence shall be submitted in the technical proposal)*** | Yes/No |
| 2 | Bidder is operating from Qatar with a local office in Qatar. ***(Evidence shall be submitted in the technical proposal)*** | Yes/No |

##### Table 1

**NOTE:** Failure to meet any mandatory criterion shall result in disqualification from the tender evaluation process.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **General Evaluation Criteria**  The Bidder will be evaluated against the following criteria and therefore Bidder should demonstrate evidence of the following  **Table 2** | | | | | |
| **Sr.No.** | **Criteria** | **Basis For Evaluation** | **Max Score** | **Minimum Passing**  **Score** |  |
| 1. | **Bidder’s understanding and response to**  **the scope of work.**  *Bidder to confirm with the following items which are to be marked with Complied/Not Complied.*   1. Deliverable 2. Detailed Scope of Work 3. Compliance Matrix Table 4. Project Management Requirements 5. Bill of Quantity (BOQ) 6. Project Plan 7. Documentation and Training 8. Delivery Terms 9. Licenses and Authority approvals 10. Service Level Agreement (SLA) 11. Non-Disclosure Agreement (NDA) 12. Contract Duration 13. Payment Method   **Individual score from section ‘a’ to ‘m’.**  (Not Acceptable = 0, Average = 0.5 to 1,  Good = 1.5, Excellent = 2)   1. **Risk Management Platform Certified against Qatar Common Criteria Scheme**   (Not Acceptable = 0, Average = 1 to 3,  Good = 3.5, Excellent = 4) | *The Bidder’s proposal shall be scored based on the criteria and scores shall be marked for each sub section ‘****a****’, to ‘****n****’.*  *Max score of this sub section a+b+c+d+e+f+g+h+i+j+k+l+m+n=* ***30***  *2 +2+ 2+2+2+2+ 2+2+2 +2+*  *2+2+2+4=* ***30***  *Minimum pass score of this sub section shall be* ***22.5***  *If all the requested information is not submitted in the technical proposal or provided information is not as per MOPH requirements and not acceptable, then score =* ***0*** | **30%** | **22.5%** |
| Page **54** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | | | | |
| 2. | **Project Resource's Qualification, relevant experience, certifications & skill set shall be provided in the bidder’s technical proposal.**   1. Implementation Team chart with their experience. **(7.5 Marks)** 2. CVs of each implementation Team member mentioning their roles **(7.5 Marks)** 3. Attach a copy of relevant certifications for each team member. **(7.5 marks)** 4. Skillset to be mentioned for design, installation, testing and rollouts. **(7.5 marks)** | The Bidder’s proposal shall be scored based on the criteria and scores shall be marked for each sub section **a, b, c & d.**  Maximum score of this sub section  *a + b + c + d =* ***30***  *7.5+7.5+7.5+7.5=* ***30***  Minimum pass score of this section shall be **22.5**  *If all the requested information is not submitted in the technical proposal or provided information is not as per MOPH requirements and not*  *acceptable, then score =* ***0*** | **30%** | **22.5%** |  |
| 3. | **Number of years in business** | *>15 years, then Score=****20%*** *13-15 years, then Score=****18%*** *5-12 years, then Score=****15%***  <*5 years, then Score=****0*** | **20%** | **15%** |
| 4. | *The bidder shall submit the* ***Project Plan*** *and* ***methodology*** *in their technical proposal as per MOPH requirements.*   1. *Detailed tasks & activities along with their dependencies.* 2. *Time and duration of each task & activity, deliverables, milestones etc.* 3. *Resources allocation to each task & activity, assumptions, and constraints.* 4. *Total duration of the Project.*   **Individual score from section ‘a’ to ‘d’.**  Not Acceptable = **0**, Average = **0.5** to **3**,  Good = **4**, Excellent = **5** | The Bidder’s proposal shall be scored based on the criteria and scores shall be marked for each sub section **a, b, c & d.**  Max score of this sub section a + b + c + d = **20**  5 + 5+ 5 + 5 = **20**  Minimum pass score of this sub section shall be **15**  If all the requested information is not submitted in the technical proposal or provided information is not as per MOPH requirements and not acceptable, then score **= 0** | **20%** | **15%** |
|  |  |  | **100%** | **75%** |
| **Note: The participant Bidder Passing score will be 75% marks.**  Page **55** of **71**  Tender Doc.: Vulnerability Assessment and Penetration Testing (VAPT) Services | | | | | |



##### Scoring

* Only those tenders which are given a total score overall reaching at least **75%** will be considered for the next evaluation stage. Bidders with a score less than **75%** will be excluded.
* The absence of a relevant description for any of Subparts listed in the above **Table 2** will automatically set the score to “0” (zero), regardless of the performance in other Subparts. Therefore, it is essential that the technical offer contains, at least, a proposal for each of the Subparts.
* Tenderers should address all the points covered by the technical specifications and show how their expertise can add value to score as many points as possible.



# Appendix A

##### Service Level Agreement (SLA)

**IMPORTANT NOTE: -THE CONTRACTUAL TERMS & CONDITIONS DEFINE THE TOTAL PENALTY TO BE NOT MORE THAN 10% OF THE CONTRACT VALUE. IN CASES WHERE THE PENALTIES, AS PER THE ABOVE SLAs, EXCEED 10% OF THE CONTRACT VALUE, THE CONTRACT WOULD BE TERMINATED**

**“No. of Days Delayed**" refers to the number of days that a certain task, or deliverable has been delayed beyond its originally agreed-upon timeline. It is to be noted that, once the SLA is breached the **“No. of Days Delayed"** includes all the calendar days. If the delays are in terms of hours, then it will be counted as a day (8 Hours = 1 Day).

##### Following SLA will be applicable to the bidder for the scope provided:

1. **Delays in deliverables from the bidder**:
   * Resources to be allocated within 5 days upon MOPH request for testing.
   * Critical findings during testing to be reported within 2 hours.
   * Report submission should be within 5 working days after testing

**Formula = 0.1%** of License cost x No of days delayed.

##### Priority Matrix

The prioritization of tickets will be as per the following Priority Matrix. The determination of **urgency** & **impact** based on business operations are made by MOPH.

***Priority Matrix***

**Impact**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **1 High** | **2 Medium** | **3 Low** |
| **1 High** | Priority 1 | Priority 2 | Priority 3 |
| **2 Medium** | Priority 2 | Priority 3 | Priority 4 |
| **3 Low** | Priority 3 | Priority 4 | Priority 5 |

**Urgency**

Any **Priority 1** incident thus identified based on the priority matrix will be termed as Major Incident. Major Incidents shall be handled as per the Major Incident Management process. All other incidents shall be handled through the regular incident management process.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Urgency** | **Description** |  | **Impact** | **Description** |
| **1**  **High** | Can no longer perform primary work functions.  Customer’s ability to works | **1**  **High** | - Any fault in the hardware/ software/application or service that results in unscheduled downtime of the |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | is severely impeded, Core business service is affected. |  |  | minimum operational system or that prevents MOPH from carrying out any planned workload that is critical to its business.   * Complete loss of functionality or the hardware/ software/application or service or system o is down * Critical/ System/service/application   failure |
| **2**  **Medium** | Some functionality is unavailable. The workaround is in place. | **2**  **Medium** | - Faults that have a major impact on the hardware/ software/application or service t but does not stop MOPH carrying out its planned workload and do not result in Unscheduled Downtime of the minimum operational system.  (Single/Multiple users) |
| **3**  **Low** | Customer is able to work, Minor Inconvenience  caused, non-urgent service. | **3**  **Low** | * Faults that do not disrupt the planned Application or Service workload and do not result in unscheduled downtime and can be worked around by the Users * Key functionality is unavailable, but a customer acceptable workaround exists and is being used or the functionality that is unavailable is non-   critical (Single user) |

In case of failure in any of the provisioned serveries, an incident ticket will be raised (in manual or automated way or via mail) and will be assigned to the concerned operations team. The ticket will be classified as per the following prioritization.

##### P1 Critical:

* Production Critical Service completely down and impacting high number of users.
* The Critical service cannot be provided as no viable or productive work around available.

##### P2 Significant:

* Incident affecting group of users.
* Production non-Critical Service completely down and not usable by limited number of users.
* Production Service completely down in non-peak hours with limited number of complaints from end users.
* Production Service with poor performance, but still the users can use it.
* Repetitive Service disconnection from time to time for short periods.
* Incident affecting organization Senior Management work.

##### P3 Medium:

* Incident with high impact on individual user.



* Incident affecting non-production services.

##### P4 Low:

* Incident with low impact on individual user.
* Incident with no operational impact.
* Request for assistance or information.

##### P5 Informational:

This category covers general inquiries or requests for information that do not cause immediate disruptions in business operations.

Such requests may involve suggestions for features, improvements, or general feedback aimed at enhancing the product or service.

Examples include Feature Suggestions, Performance Enhancement, Cosmetic Improvements, General Queries.



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Level** | **P1** | **P2** | **P3** | **P4** | **P5** |
| **Support Window** | **24X7** | **24X7** | **8X5** | **8X5** | **8X5** |
| **Response Time Target** | Within 15 Minutes | Within 15 Minutes | Within 30 Minutes | Within 30 Minutes | Within 30 Minutes |
| **Penalty for SLA breach of Response Time** | 0.27 % of total support cost. | 0.22% of total support cost. | 0.16 % of total support cost. | 0.11 % of total support cost. | 0.11% of total support cost. |
| **Resolution Time** | Within 2 Hours | Within 3 Hours | Within 8 Hours | Within 24 Hours | Within 24 Hours |
| **Total fix Time** | Within 2 Hours  15 Minutes | Within 3 Hours  15 Minutes | Within 8 Hours  30 Minutes | Within 24 Hours  30 Minutes | Within 24 Hours  30 Minutes |
| **Penalty for SLA breach for Total Fix time** | **0.54%** of total support cost for the 1st hour of breach. Then **QR 500** for each extra hour. | **0.44 %** of total support cost for the 1st hour of breach. Then **QR**  **400** for each extra hour. | **0.27%** of total support cost for the 1st hour of breach. Then **QR 150** for each extra hour. | **0.16%** of total support cost for the 1st hour of breach. Then **QR 150** for each extra hour. | **0.16 %** of total support cost for the 1st hour of breach. Then **QR**  **100** for each extra hour. |
| **Incident Occurrence allowed (If exceeds will lead to Contract Termination)** | <=3 tickets per quarter. | <=3 tickets per quarter. | <=5 tickets per quarter. | <=5 tickets per quarter. | <=5 tickets per quarter. |
| **Penalty for SLA breach for Incident Occurrence** | 0.5 % of total support cost for every new incident apart  from the allowed. | 0.4 % of total support cost for  every new incident apart from the allowed. | 0.3 % of total support cost for every new incident apart  from the allowed. | 0.2 % of total support cost for  every new incident apart from the allowed. | 0.1 % of total support cost for  every new incident apart from the allowed. |

**Response Time**: Time from incident logged till the time the support engineer accepted the ticket. **Resolution Time**: Time from the incident logged till the time the support engineer resolved the issue. **Total Fix Time:** Response Time + Resolution Time.



# Appendix B

##### NON- DISCLOSURE AGREEMENT

The below NDA at individual consultant level should be signed after the contract is awarded. This non — disclosure agreement (“Agreement”) is made between the Vendor staff and MOPH.

To perform their job duties in support of this project, vendor employees in Information Systems (IS) application support roles are frequently provided privileged access to the information systems that they support and to the data and records managed by those systems. Privileged access imposes upon the Vendor IT support employee, the responsibility and obligation to use that access in an ethical, professional, and legal manner that is strictly within his or her authorized job functions. MOPH is committed to advancing the ethical and responsible use of all information resources and does not tolerate illegal, dishonest, improper, or irresponsible use.

For all the MOPH provided access login credentials, the vendor resources are required to maintain the integrity. Not to share any of these credentials with anyone even with colleagues working in the same project. Each vendor IT resource to use his or her own login credentials. The same applies for any VPN access credentials. Further, no VPN access for MOPH network is provided from Egypt, UAE, Saudi Arabia & Bahrain.

RECITALS

* Access to computer desktops/ laptops and applications is bound by MOPH IS department related policies.
* VPN access for remote access to MOPH systems

##### AGREEMENT

In exchange for the elevated access privileges granted to me to support MOPH projects / applications, I agree to abide by the following performance standards:

1. To take every reasonable precaution to prevent unnecessary or unauthorized access to any passwords, user identifications, or other information that may be used to access information systems, whether those systems belong to the MOPH or to private parties.
2. To limit access to the information contained or obtained from information systems to authorized persons.
3. To treat all information encountered in the performance of my duties as confidential.
4. To seek guidance from my supervisor in MOPH whenever I am unsure of the correct decision regarding the appropriate use and confidentiality of information, and to do so BEFORE I take any action that might compromise that use or confidentially.
5. TO avoid any sharing, recording transmission, alteration, or deletion of information in the information systems expect as required in performance of my job duties.
6. To strictly comply with all the MOPH’s IS policies related to the use and security of the MOPH’s information

resources.

1. To report any incidents of non –compliance with the terms of this agreement to my supervisor.



I understand that this agreement applies to the MOPH network, all electronic systems owned or operated by MOPH, whether or not they are connected to that network, and to all privately owned electronic systems that may be brought and connected to the MOPH network.

I further understand that the MOPH considers violation of these standards to be serious offense, and that if I violate this agreement; I may be subjected to disciplinary action according to MOPH bylaws.

Vendor Employee Signature:

Printed Employee Name:

Employee Title:

Company / Vendor Name:

Date:

**Vendor Company Stamp**



**SUPPLY/SERVICE ORDER FORM**

**CONTRACT No. : MOPH/TAC/IT/072/2025**

**CONTRACT TITLE: VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) SERVICES**

#### Supply Order No.

TO CONTRACTOR:

Cost Center: Location: Date:

You are hereby instructed to perform the following specified SERVICES and supply the following GOODS in accordance with the terms and conditions of the captioned CONTRACT. Please sign this form at the space provided below and return a copy to MOPH’s REPRESENTATIVE immediately.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sr. No.** | **Description** | **Unit** | **Quantity** | **Cost (QR)** |
|  |  |  |  |  |
| **SO Value:** | | | |  |

|  |  |  |
| --- | --- | --- |
| **SO Date (Date/Time)** | **DELIVERY DATE**  **(Date/Time)** | **ACTUAL DELIVERY DATE**  **(Date/Time)** |
|  |  |  |
| Remarks/Special Instructions\*\*: | | |

##### CHECKLIST (Post Completion)

Total delay (if applicable) – Deduction for delayed SERVICE (QR.)

**Total amount to be recovered (QR**.**)**

|  |
| --- |
| Amount approved for payment QR. |
| Remarks (Post Completion)\*\* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ON SERVICE COMPLETION:** | | |  | | |
| **For MOPH** | Initiated by: | Approved by: | | Inspected by: | Approved by: |
| Signed: |  |  | |  |  |
| Name: |  |  | |  |  |
| Position Staff  number. |  |  | |  |  |
| CONTRACTOR’s  Acceptance: |  | | | | |

Invoice No. (To be filled by CONTRACTOR):

\* Starts with CONTRACT No. followed by



**الملحق (ṿ) جدول الأسعار**

**Annex B Schedule of Prices**

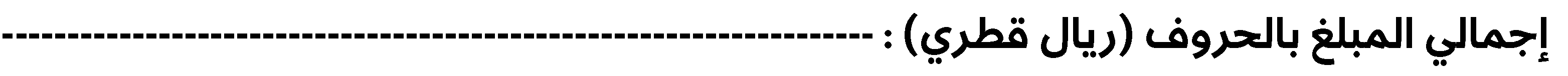


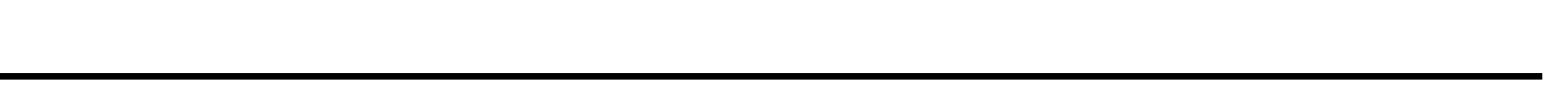
**الأسعار**

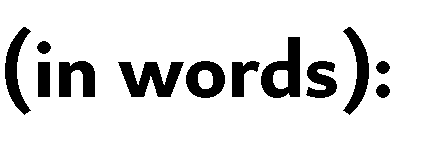
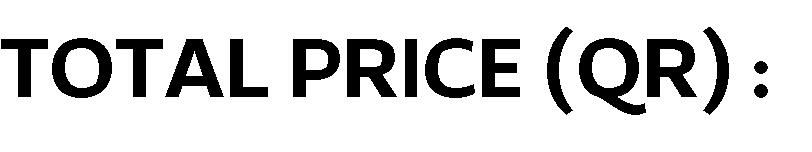
## Schedule of Prices

(أ) الملحق يف . المذكور الأعمال لنطاق وفقا الأسعار جدول Schedule of Prices as per Scope of Work stated in Annex A

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SN** | **Product/Service Descriptions** | **UoM** | **Quantity** | **Unit Price**  **(QR)** | **Total Price**  **(QR)** |
| **1** | Project Kick Off/Initiation | Lot | 1 |  |  |
| **2** | Year 1 scope, Vulnerability Assessment and Penetration  Testing (VAPT), Documentation/Reports/Presentation/Revalidation | Lot | 1 |  |  |
| **3** | Year 2 scope, Vulnerability Assessment and Penetration Testing (VAPT), Documentation/Reports/Presentation/Revalidation | Lot | 1 |  |  |
| **4** | Year 3 scope, Vulnerability Assessment and Penetration Testing (VAPT), Documentation/Reports/Presentation/Revalidation | Lot | 1 |  |  |
| **Grand Total** | | | |  | |









**المرفقات:**

## .1نموذج الشية وعدم الإفصاح. .2 نموذج التأم ·ي النها ين.



#### وزارة وزارة الصحة العامة نموذج الشية وعدم الافصاح

**Non-Disclosure Agreement**

This Non-Disclosure Agreement (“Agreement”) is entered into this ----------------day of -----------, 2025, between the Ministry of Public Health (“MOPH”) and, , (“Tenderer”) having a business address at .

##### Whereas:

1. MOPH and Tenderer wish to exchange certain information pertaining to the below stated purpose. This exchange includes all communications of information between the parties in any form whatsoever, including oral, written and machine-readable form.
2. Each party regards certain parts of the information it possesses to be secret and desires to protect those parts from unauthorized disclosure or use (such as secret parts being hereafter collectively referred to disclose information (as “Disclosing Party”) and receive information (as “Receiving Party”) on the terms and conditions set forth herein.

##### Article 1

* 1. “CONFIDENTIAL INFORMATION” as used herein, means this Agreement and all information which Receiving Party, directly or indirectly, acquires from Disclosing Party or its Affiliates or any other information concerning the technical and business activities and know-how of Disclosing Party or its Affiliates, except information falling into any of the following categories:

1. Information, which prior to the time of disclosure or acquisition hereunder, is in the public domain;
2. Information which, after disclosure or acquisition hereunder, enters the public domain, except

where such entry is the result of Receiving Party’s breach of this Agreement;

1. Information, other than that obtained from third parties, which prior to disclosure or acquisition hereunder, was already lawfully in Receiving Party’s possession either without limitation on disclosure to others or, which subsequently becomes free of such limitation;
2. Information obtained by Receiving Party from a third party who is lawfully in possession of such information and not subject to a contractual or fiduciary relationship with Disclosing Party or any of its Affiliated or another with respect to said information. Receiving Party may use and disclose such information in accordance with the terms under which it was provided by such as third party.
   1. CONFIDENTIAL INFORMATION shall not be deemed to be within the foregoing categories merely because such information is embraced by more general information lawfully in the public domain or in



Receiving Party’s possession. In addition, any combination of features shall not be deemed to be within the foregoing categories merely because individual features are in the public domain or in Receiving Party’s possession but only if the combination itself and its principle of operation are lawfully in the public domain or in Receiving Party’s possession.

* 1. Receiving Party represents that it has a policy and procedure designed to protect trade secret rights of its own proprietary information, including notices to its employees to prevent unauthorized publication and disclosure of such information. Receiving Party agrees that CONFIDENTIAL INFORMATION shall be subject to such policy and procedure. In addition, Receiving Party agrees that it shall not disclose any INFORMATION other than on Disclosing Party’s behalf except as Disclosing Party may otherwise authorize in writing. If disclosure to a third party is so authorized, Receiving Party shall enter into a confidentiality agreement with the said party containing the same terms and conditions with respect to use or disclosure of CONFIDENTIAL INFORMATION as this Agreement contains.

##### Article 2

The Receiving Party may use the CONFIDENTIAL INFORMATION solely for the purpose of the Project and/or

Services described in the Contract documents (“Purpose”).

##### Article 3

The Receiving Party will:

1. (1) Not disclose information of Disclosing Party to any other person and (2) use at least same degree of care to maintain the information confidential as Receiving Party uses in maintaining as confidential its own information, but always at least a reasonable degree of care;
2. Use the information only for the above purpose;
3. Restrict disclosure of the information of the Disclosing Party solely to those employees of Receiving Party having a need to know such information in order to accomplish the purpose stated above;
4. Within fifteen (15) days following request of Disclosing Party return to the Disclosing Party all documentation, copies, notes, diagrams, computer memory media and other materials containing any portion of the information, or confirm to Disclosing Party, in writing, the destruction of such materials.

##### Article 4

The information shall remain the sole property of Disclosing Party.

##### Article 5

Disclosing Party shall not make any representation with respect to and does not warrant any information provided under this Agreement but shall furnish such in good faith. Without restricting the generality of the foregoing, Disclosing Party shall not make any representations nor warranties, whether written or oral, statutory, express or implied with respect to the information which may be provided hereunder, including without limitation, any warranty of merchantability or of fitness for a particular purpose.

Neither Disclosing Party shall be liable for any special, incidental nor consequential damages of any nature whatsoever resulting from receipt or use of the information by the Receiving Party.



##### Article 6

In the event of a breach or threatened breach or intended breach of this Agreement by either party, the other party, in addition to any other rights and remedies available to it at law or in equity, shall be entitled to preliminary and final injunctions, enjoining and restraining such a breach or threatened breach or intended breach.

##### Article 7

The validity, construction, and performance of this Agreement are governed by the laws of the State of Qatar.

##### Article 8

This Agreement shall continue from the date written below until terminated by either party by giving thirty (30) days written notice to the other party of its intent to terminate this Agreement. Notwithstanding such termination, the obligations of the Receiving Party concerning confidentiality shall terminate five (5) years following receipt of the CONFIDENTIAL INFORMATION.

##### Article 9

This Agreement is binding upon both parties and upon the directors, officers, employees and agents of each.

##### Article 10

The parties hereto are independent Tenderers. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferrable.

##### Article 11

If any term of this Agreement shall be held to be illegal or unenforceable by a court of competent jurisdiction, the remaining terms shall remain in full force and effect.

##### Article 12

This Agreement may be modified only by writing signed by duly authorized representatives of both parties.

##### Article 13

This Agreement represents the entire agreement of the parties hereto pertaining to the subject matter of this Agreement and supersedes any and all prior oral discussions and/or written correspondences or agreements between the parties with respect thereto all of which are excluded.

**IN WITNESS WHEREOF**, the parties have executed this Agreement as of the date last written below:

##### For MOPH For Tenderer

By Name Title Date

|  |  |  |  |
| --- | --- | --- | --- |
| : |  | By : |  |
| : |  | Name : |  |
| : |  | Title : |  |
| : |  | Date : |  |



## نموذج خطاṿ التأم ·ي النها ين بموجب القواعد الموحدة 758 URDG

نوع خطاب الضمان: )حدد خطاب الضمان , خطاب ضمان دفعه مقدمه او خطاب ضمان حسن التنفيذ او خطاب ضمان دفع او خطاب ضمان منجزات او غ ته .(

رقم خطاب الضمان: )ادخل رقم مرجع خطاب الضمان(. الضامن : )ادخل الاسم وعنوان مكان الإصدار(

طالب الإصدار : )ادخل الاسم والعنوان(

المستفيد: )ادخل الاسم والعنوان(

الأساسية: ال ر .تامات طالب الإصدار فيما يتعلق ب )ادخل رقم مرجع او ايه معلومة تعرف بالعقد او ب رسروط العلاقة المناقصة او ايه علاقة ب .ي طالب الإصدار والمستفيد وال ر ين على أساسها يرتكز خطاب الضمان(

قيمه وعمله خطاب الضمان : )ادخل الحد الأقص القابل للدفع بالأرقام والكلمات والعملة ال ر ين سيدفع فيها(

أي مستند مطلوب لدعم المطالبة بالدفع: لايوجد غ ت الإفادة الداعمة )تصريــــح المستفيد بالإشارة ال كيفية اخلال طالب الضمان بال ر .تاماته( المطلوبة صراحه . يف النص ادناه.

)أضف أي مستند اخر مطلوب لدعم المطالبة بالدفع. . يف حاله لم يطلب خطاب الضمان مستندات أخرى ماعدا المطالبة والإفادة الداعمة، اب ر يف هذا المكان فارغا واذكر "لا يوجد ."

لغة ايه مستندات مطلوبة: )ادخل اللغة لاي مستندات مطلوبة. ان المستندات ال ر ين تصدر عن طالب الإصدار او المستفيد ال ر ين تصدر عن طالب الإصدار او المستفيد ستكون بلغه خطاب الضمان ما لم يذكر خلاف ذلك هنا(

شكل المطالبة: )ادخل بشكل ور ر يف او الك رتو . ين. إذا كان ورقيا، حدد طريقه التسليم. إذا كان الك رتونيا، حدد الشكل والنظام الذي سيستخدم لتسليم البيانات والعنوان الالك رتو . ين للتقديم.(

مكان تقديم المطالبة: ) على الضامن ان يدخل عنوان الفرع الذي سيتم تقديم المطالبة الخطية اليها و . يف حال التقديم الالك رتو . ين ، العائد للضامن. . يف حال عدم تحديد مكان المطالبة يعت .ت مكان اصدار خطاب الضمان هو مكان المطالبة .(

الانتهاء: )ادخل تاريــــخ انتهاء( ............... **7**) **أيام عمل بعد إتمام تنفيذ العقد بما · يف ذلك مدة الضمان والصيانة**(

الطرف المسؤول عن دفع ايه مصاريف : ) ادخل اسم هذا الطرف .(

انناكضامن نتعهد ها هنا بشكل غ ت قابل للنقض ودون الاعتداد باي معارضه أياكانت بان ندفع للمستفيد أي مبلغ لغايه قيمه خطاب الضمان عند قيام المستفيد بتقديم مطالبه مطابقه بذلك مع ادراج مرجع او اشاره خطاب الضمان، مستوفيه ل رسروط خطاب الضمان وفقا للنموذج المحدد أعلاه , على ان تكون المطالبة المذكورة مدعومة باي مستندات أخرى قد تكون محدده . يف م ر .ي خطاب الضمان ,

و . يف أي حال من الأحوال مدعومة بتصريــــح المستفيد سواء كان هذا التصريــــح . يف المطالبة نفسها او . يف مستند منفصل وموقع يكون

مرفقا مع او يش ت ال المطالبة ، يب .ي فيه وجه او أوجه اخفاق طالب اصدار خطاب الضمان بال ر .تاماته بموجب العلاقة الأساسية .

يجب ان تسلم أي مطالبه بموجب خطاب الضمان هذا الينا . يف او قبل تاريــــخ الانتهاء . يف مكان التقديم المشار اليه أعلاه

خطاب الضمان هذا خاضع للقواعد الموحدة لخطابات الضمان تحت الطلب (URDG) تنقيح ,2010



منشور غرفه التجارة الدولية رقم 758

المادة (5) من القواعد الموحدة لخطابات الضمان عند الطلب كتيب رقم 758 تنص على ما ي يلى : استقلاليه خطاب الضمان وخطاب الضمان المقابل

أ. خطاب الضمان بطبيعته مستقل عن العلاقة الأساسية، وعن طلب الإصدار ، والضامن غ ت مع . ين او ملزم باي حال من الأحوال بمثل هذه العلاقة الأساسية ان الإشارة . يف خطاب الضمان ال العلاقة الأساسية بغرض التعريف بها لا يغ ت من الطبيعية المستقلة لخطاب الضمان . تعهد الضامن بالدفع بموجب خطاب الضمان لا يخضع لادعاءات او دفوع ناشئة عن ايه علاقه غ ت العلاقة ما ب .ي الضامن والمستفيد كما يه محدده . يف خطاب الضمان .