# UCO BANK

## Department of Information Technology

**Request for Proposal for Implementation of Anti-Phishing Managed Services.**
**(Ref No.: UCO/DIT/590/2016-17 dated 04-07-2016)**

**Replies / Corrigendum / Addendum**
**Ref. No. UCO/DIT/764/2016-17 Date: 28-07-2016**

| | |
|---|---|
| **Last Date & Time of Submission of Bids Extended upto** | **10-08-2016 15:00 Hours** |

**Please treat this Addendum / Clarifications as an integral part of the RFP document issued. No further queries pertaining to this Addendum / Clarifications or the RFP will be entertained.**
**All other terms and conditions remain unchanged.**

**Date: 28-07-2016**

**UCO BANK**

**Department of Information Technology**

**Request for Proposal (RFP) For RFP for Implementation of Anti-Phishing Managed Services RFP REF NO: UCO/DIT/590/2016-17 Date 04/07/2016 Pre-Bid Responses/ Clarifications to Queries raised by the Bidder(s), Amendments, Addendums and Corrigendum's**

| SL. No | Page no | Clause No | Terms &Conditionsas per RFP | Queries/Suggestions by the Bidder (s) | Bank's Response (s) |
|---|---|---|---|---|---|
| **1** | 18 | 4.1.2 | The bidder should ensure bringing down the reactivated phishing site at earliest which was earlier detected as phishing site. If the same site becomes active again within a period of 180 days of its taking down, it should not be treated as a new incident and should be taken down as part of original incident | Assumption is "same site" refers to the same URL as previously detected. Please confirm. | Same Site refers to same domain name. |
| **2** | 19 | 4.1.9 | Monitor spoofed email ids that may be used for sending emails to the customers of the Bank. | Please confirm if this means that the service provider has to identify the email address used for sending spam emails to the customer. This is primarily catered by Anti-Spam solution and falls beyond the scope of Anti-Phishing. | Monitoring spoofed email ids must be part of the solution in offering. |
| **3** | 20 | 4.1.7 | Brand Abuse cases | Our assumption is the brand abuse is relative to the Phishing websites where UCO Bank's brand is represented. Please confirm. | Yes |

| | | | | | |
|---|---|---|---|---|---|
| **4** | 20 | 4.1.19 | Alternative response mechanisms other than web site take down to minimize impact of phishing. | What kind of alternate mechanism is sought? | Any alternative response mechanism (other than website take down) should be used to minimize impact of phishing. |
| **5** | 19 | 4.1.6 | Monitor web-server referrer logs and implementation of tools for referrer log analysis of web server | Details of web server required to check the feasibility and compatibility with our web referral monitoring tool | Will be shared with the successful bidder. Successful bidder has to make it feasible and compactable with their tool. |
| **6** | 43 | Annex ure-G | Details of web server required to check the feasibility and compatibility with our web referral monitoring tool | Assuming Bank will provide Secured Connectivity between HCL SOC and UCO Bank, Bank to provide server (if require) for Web Referral logs in the Web server and related OS, Storage. | RFP clause stands.<br>Bidder has to take care of all types of infrastructure cost required for establishing web referral monitoring tools. |
| **7** | 18 | 4.1.5 | Track hosting of phishing sites through digital watermark. Phishing sites must be tracked using digital watermark. | The solution what we are proposing is not capable of digital watermarking, hence request the Bank to remove the clause. | Phishing sites must be tracked using digital watermark or equivalent or higher technology |
| **8** | 21 | 5.4 | Bank shall pay take down charges on per site basis and there shall be no minimum charges commitment from the Bank | Would request the bank to consider a minimum take down commitment for10 takedown per year. | RFP Clause Stands. No minimum commitment from Bank. |
| **9** | 19 | 4.1.13 | Selected bidder should assist the Bank for co-ordinate with law enforcement agencies like CERT-IN, Banking Ombudsman etc. | Kindly freeze the scope of assistance required limited to Anti-Phishing solution only. | Coordination with low enforcement agencies limited to Anti-Phishing solution only. |

| | | | | | |
|---|---|---|---|---|---|
| **10** | | 4.2.1 | The solution should monitor Website for 24x7 basis for any breach of (Confidentiality & Integrity) | Solution DD is planning to purpose, can scan website every 30 minutes. Hence Bank is requested to change the clause" The Solution should monitor Websites for 24x7 basis for any breach of (Confidentiality & Integrity) in every 30 minutes" as per the best practices being followed by all other Banks. | RFP Clause Stands. |
| **11** | | 4.2.2 | 24x7 monitoring/ scanning of web pages for real-time detection of malware Injection. No skipping of page scanning. | Solution DD is planning to purpose, can scan website every 30 minutes. Hence Bank is requested to change the clause" The Solution should monitor Websites for 24x7 basis for any breach of (Confidentiality & Integrity) in every 30 minutes" as per the best practices being followed by all other Banks | RFP Clause Stands. |
| **12** | | 4.2.4 | Solution should proactively inform Bank about potential threats/ vulnerabilities, new threats in circulation. | Is Bank looking for just outside knowledge or want to do application PT test to find vulnerability of websites? Need more clarification on this. | Bank to be proactively informed. |
| **13** | | 4.2.10 | SQL Injection/Cross-site scripting | Malware scanning can report malware or any malicious content. Is Bank's expectation is to detect SQL and XSS Vulnerabilities in the website? If yes, what is the periodicity of the Automated Application Security Scanning? Scanning expected? Is bank looking for any manual App PT also? | Bank's expectation is to detect SQL and XSS Vulnerabilities in the website.<br>Automated Application Security Scanning on quarterly basis. |

| | | | | | |
|---|---|---|---|---|---|
| **14** | 25 | 5.12 | Indemnity | RFP at various places requires bidders to indemnify and the indemnification obligation is very broad and without providing the detailed and established norms for indemnification. To make the contract reasonable and commercially viable as per standard practice observed within the industry, we request that the clarity be provided in the agreement that Indemnity shall only be restricted to third party claim (i) IPR Infringement indemnity, (ii) bodily injury and death and tangible property damage due to gross negligence and willful misconduct, (iii) Confidentiality claims. The process of indemnification shall provide the requirement of notice, right to defend and settle and the concept of apportionment (liable only to the extent of its claim), mitigation and carve-outs. | RFP clause stands. |
| **15** | 15 | 1.21 | Indemnity | RFP lacks clarity on entire liability of bidder under this RFP. Bidder requests that clarity be brought by including following limitation of liability clause in the RFP: "Neither Bank nor the Vendor shall in any event be liable for indirect and consequential loss and damages including but not limited to loss of business, anticipated revenue, loss of profit etc. To the extent allowed by laws in India, the liability of each party under this agreement, in any event regardless of nature of claim under contract, torts and other theory shall be limited to the total contract value under the purchase order. | RFP clause stands. |

| | | | | | |
|---|---|---|---|---|---|
| **16** | 22 | 5.6 | Inspection & Audit | Bidder requests that any audit by Bank shall be subject to certain security and confidentiality restrictions applicable to Bidder's premises or other client's data. | Security and confidentiality restrictions applicable to bidder's premises or other client's data,will be as per the industry standard. |

All other terms & conditions remain unchanged.

## Commercial Bid(Revised)

| S.N. | Major Activities | Amount for Three Years exclusive of all taxes (in Rs.) (A) | Taxes at present rate* (in Rs)(B) | Total Cost (in Rs.) C=(A+B) |
|---|---|---|---|---|
| 1 | 24x7X365 Phishing monitoring | | | |
| 2 | Implementation of real time phishing detection mechanisms and alerts | | | |
| 3 | Taking down charges per site. | | | |
| 4 | Monitoring similar domain name registration | | | |
| 5 | Monitoring spam traps to detect Phishing mails | | | |
| 6 | Web site analysis to detect Phishing sites | | | |
| 7 | Alternative response mechanisms other than web site take down to minimise impact of phishing | | | |
| 8 | Benchmarking of bank's internet banking site and suggest controls required to minimise impact from phishing attacks | | | |
| 9 | Automated Application Security Scanning on quarterly basis | | | |
| 10 | Anti malware services for UCO Bank's websites **(20 sites)** | | | |
| **Total cost of Ownership (TCO) (Inclusive of all the Taxes)** ***(Amount quoted in figures)*** | | | | |
| **Total cost of Ownership (TCO) (Inclusive of all the Taxes)** ***(Amount quoted in words)*** | | | | |

**Place:**

**Date:**

**AUTHORISED SIGNATORY**

**Name:**

**Designation:**

**Notes**

1. Bank shall pay take down charges on per site basis and there shall be no minimum charges commitment from the Bank. Take down charges per site shall be arrived by dividing the rates quoted in item no. 3 above by 150.
2. If the same site becomes active again within a period of 180 days of its taking down, it should not be treated as a new incident and should be taken down as part original incident.
3. * Bank will pay all types of applicable taxes (including Service tax) ruling at the time of services rendered and the resultant billing.
4. Bidders to strictly quote in the format and for periods as mentioned above.
5. No counter condition/assumption in response to commercial bid will be accepted. Bank has a right to reject such bid
6. UCO bank reserves the right to add more websites of the Bank during the contract period at the same rate quoted by the bidder for "Anti malware services".
7. UCO Bank reserves the right to derive the per site cost from the above cost of 20 websites.
8. The selected Bidder has to keep the finalized price valid during the contract period. There should not be any escalation due to fluctuation in taxes, foreign currency or change in duty structure or for any other reasons. However, impact of fall in prices, taxes, duties or any other external factors like downward movement of foreign exchange rates etc. would be passed on to The Bank suo moto.