



THE BANK OF KHYBER

INVITATION TO BID

The Bank of Khyber invites sealed bids from Courier/ Dispatch Companies for “Dispatch of Half Yearly Statement of Accounts” to meet State Bank of Pakistan (SBP) Standing Operating Procedure (SOP’s) for the selection/ minimum requirements required to be fulfilled by the service providers.

SERVICE TYPE:

- Paper (Account Statement): A-4, 80-90 gram, color printing, preprinted with Bank Logo & advertisement (As per approved specimen)
- Printing: Digital Printing in Black & White on high speed digital printers on one side of paper.
- Envelopes: Machine made imported envelopes in DL size as per approved design 4 color printing of Bank’s logo on one side for automated stuffing.
- Automated stuffing: Automatic stuffing of Account Statements (Multiple Pages)
- Distribution: Nationwide delivery service through courier. Non service area shipments will be delivered through GPO.

The Courier/ Dispatch Company should follow the following SOPs as per SBP/ PBA guidelines.

PROCESS FLOW:

- Statement of Account data extracted at Bank’s end.
- A password protected file containing extracted data for SOA is shared in a SFTP (Secured File Transfer Protocol with the service provider)
- Service provider shares and dispatching of the SOAs, Service Provider sends the “Booking File” to Bank.
- After execution of dispatching exercise, the service provider shares the delivery status i.e. delivered/ undelivered.
- The undelivered statements are sent by service provider to relevant branches.
- Upon receipt of un-delivered SOA’s, the same are reconciled by bank against the delivery status file received from service provider to ensure that all undelivered consignments have been received by the Bank.
- After 90 days from the completion of the SOA dispatch exercise, the data is destroyed by service provider from their servers and in this regard a Data Destruction Certificate is obtained from Service Provider.

CONTROL MEASURES TO ENSURE CUSTOMER DATA PROTECTION:

In order to mitigate the risk of data leakage or exploitation, following control measures ensured to be in place at the Service Provider’s end:

- Non-Disclosure Agreement (NDA) with the service provider is to be signed. The NDA must be verified and vetted by the Legal Department to ensure that it covers all aspects to the risks of data secrecy and to ensure that it is compliant with SBP outsourcing guidelines and other regulatory instructions.
- The data file is password protected and is shared with the service provider

though a Secured File Transfer Protocol (SFTP). It is ensured that the SFTP mechanism with the service provider has following security & access controls:

- a. Access restricted to authorize IP only.
 - b. High complexity of the Password.
 - c. Account lockout policy is in place.
 - d. The SFTP is protected against possible Denial of Service (DoS) attack
- The Service Provider at minimum, has following network security controls in place:
 - a. Segregated LAN (VLANs)
 - b. No public interface or application
 - c. Restricted IPs & ports with privileges
 - d. Isolated network
 - The service provider, at minimum, has following information security controls in place:
 - a. Access control policy and procedure
 - b. Web upload protection
 - c. USB mass storage device protection
 - d. Print screen protection
 - e. Software instantiation restrictions
 - f. FTP/ SFTP upload protection
 - g. Patch management
 - h. Firewall policies to restrict inter-VLAN communication
 - i. Outward e-mail access to registered addresses only.
 - Accordingly, the service provider should have international certifications with respect to the information security and process quality preferably ISO 27001:2005 & ISO 9001:2008 respectively.
 - The vendor should carry out complete printing and stuffing of statements at its own facility.
 - The facility should be restricted to any kind of unauthorized access.
 - The main access to the facility should be protected by bio matric access system.
 - A security guard should be posted at the main entrance of the facility to ensure that no kind of physical data is moved out without proper approvals.
 - The process cycle of service provider, from data uploading to printing, stuffing and storage areas.
 - CCTV surveillances cameras should be installed inside and on the main entrance of the facility to cover and monitor printing, stuffing and storage areas.
 - The data is destroyed by the service provider within 90 days of the completion of printing job. The destruction certification should be obtained in this regard.
 - The service provider has obtained undertaking with regards to data secrecy and non-disclosure of information, from its employees engaged in this activity.
 - The service provider should ensure that the whereabouts of the employees working in the facility and their CNICs have been verified. The record of such verification must be maintained by them.

- Those interested shall submit their quotations in sealed envelopes along with security deposit equivalent to 2% of total number of Half Yearly Statement of Accounts which is 336,911 approximately, and a copy of Income Tax registration certificate on May 16, 2017 at 11:00 a.m at The Bank of Khyber, General Administration Division, 29-A, The Mall, Peshawar Cantt.
- The bidders are requested to quote their best and final prices as any negotiation will not be admissible.
- The bids will be opened on same date at 11:30 a.m
- The bidders are requested to quote their best and final prices as any negotiation will not be admissible.
- Pre-bid documents are available on BoK website.
- The firm should be income tax and sales tax registered.

Note: This Contract will be for a period of 2 years from the date of submission of order/ agreement and quoted rates should remain the same during these two years.

Bids will be opened in the presence of bidders or their representatives.

Head General Administration Division

The Bank of Khyber

29-A, The Mall

Peshawar Cantt. Tel: 091-5279687



THE BANK OF KHYBER

INVITATION TO BID

The Bank of Khyber invites sealed bids from Courier/ Dispatch Companies for “Dispatch of Half Yearly Statement of Accounts” to meet State Bank of Pakistan (SBP) Standing Operating Procedure (SOP’s) for the selection/ minimum requirements required to be fulfilled by the service providers.

SERVICE TYPE:

- Paper (Account Statement): A-4, 80-90 gram, color printing, preprinted with Bank Logo & advertisement (As per approved specimen)
- Printing: Digital Printing in Black & White on high speed digital printers on one side of paper.
- Envelopes: Machine made imported envelopes in DL size as per approved design 4 color printing of Bank’s logo on one side for automated stuffing.
- Automated stuffing: Automatic stuffing of Account Statements (Multiple Pages)
- Distribution: Nationwide delivery service through courier. Non service area shipments will be delivered through GPO.

The Courier/ Dispatch Company should follow the following SOPs as per SBP/ PBA guidelines.

PROCESS FLOW:

- Statement of Account data extracted at Bank’s end.
- A password protected file containing extracted data for SOA is shared in a SFTP (Secured File Transfer Protocol with the service provider)
- Service provider shares and dispatching of the SOAs, Service Provider sends the “Booking File” to Bank.
- After execution of dispatching exercise, the service provider shares the delivery status i.e. delivered/ undelivered.
- The undelivered statements are sent by service provider to relevant branches.
- Upon receipt of un-delivered SOA’s, the same are reconciled by bank against the delivery status file received from service provider to ensure that all undelivered consignments have been received by the Bank.
- After 90 days from the completion of the SOA dispatch exercise, the data is destroyed by service provider from their servers and in this regard a Data Destruction Certificate is obtained from Service Provider.

CONTROL MEASURES TO ENSURE CUSTOMER DATA PROTECTION:

In order to mitigate the risk of data leakage or exploitation, following control measures ensured to be in place at the Service Provider’s end:

- Non-Disclosure Agreement (NDA) with the service provider is to be signed. The NDA must be verified and vetted by the Legal Department to ensure that it covers all aspects to the risks of data secrecy and to ensure that it is compliant with SBP outsourcing guidelines and other regulatory instructions.

- The data file is password protected and is shared with the service provider through a Secured File Transfer Protocol (SFTP). It is ensured that the SFTP mechanism with the service provider has following security & access controls:
 - a. Access restricted to authorize IP only.
 - b. High complexity of the Password.
 - c. Account lockout policy is in place.
 - d. The SFTP is protected against possible Denial of Service (DoS) attack
- The Service Provider at minimum, has following network security controls in place:
 - a. Segregated LAN (VLANs)
 - b. No public interface or application
 - c. Restricted IPs & ports with privileges
 - d. Isolated network
- The service provider, at minimum, has following information security controls in place:
 - a. Access control policy and procedure
 - b. Web upload protection
 - c. USB mass storage device protection
 - d. Print screen protection
 - e. Software instantiation restrictions
 - f. FTP/ SFTP upload protection
 - g. Patch management
 - h. Firewall policies to restrict inter-VLAN communication
 - i. Outward e-mail access to registered addresses only.
- Accordingly, the service provider should have international certifications with respect to the information security and process quality preferably ISO 27001:2005 & ISO 9001:2008 respectively.
- The vendor should carry out complete printing and stuffing of statements at its own facility.
- The facility should be restricted to any kind of unauthorized access.
- The main access to the facility should be protected by bio matric access system.
- A security guard should be posted at the main entrance of the facility to ensure that no kind of physical data is moved out without proper approvals.
- The process cycle of service provider, from data uploading to printing, stuffing and storage areas.
- CCTV surveillances cameras should be installed inside and on the main entrance of the facility to cover and monitor printing, stuffing and storage areas.
- The data is destroyed by the service provider within 90 days of the completion of printing job. The destruction certification should be obtained in this regard.
- The service provider has obtained undertaking with regards to data secrecy and non-disclosure of information, from its employees engaged in this activity.
- The service provider should ensure that the whereabouts of the employees working in the facility and their CNICs have been verified. The record of such verification must be maintained by them.

➤ Those interested shall submit their quotations in sealed envelopes along with security deposit equivalent to 2% of total number of Half Yearly Statement of

Accounts which is 336,911 approximately, and a copy of Income Tax registration certificate on May 16, 2017 at 11:00 a.m at The Bank of Khyber, General Administration Division, 29-A, The Mall, Peshawar Cantt.

- The bidders are requested to quote their best and final prices as any negotiation will not be admissible.
- The bids will be opened on same date at 11:30 a.m
- The bidders are requested to quote their best and final prices as any negotiation will not be admissible.
- Pre-bid documents are available on BoK website.
- The firm should be income tax and sales tax registered.

Note: This Contract will be for a period of 2 years from the date of submission of order/ agreement and quoted rates should remain the same during these two years.

Bids will be opened in the presence of bidders or their representatives.

Head General Administration Division

The Bank of Khyber

29-A, The Mall

Peshawar Cantt. Tel: 091-5279687