Madam/ Dear Sir,

Sub: Password protected for Drafting of new policies and Review and gap assessment policy

PURPOSE: To engage firm, which has the capability and experience of Risk Assessment, ISO 27001/ Security services/ Policy formation/ Gap assessment of Cyber Security frame work June 2016 in banking sector for following scope of work.

1. Drafting for formulation of Information Security Policy- Scope as per Annexure II
2. Drafting for formulation of an exception policy for handling instances of noncompliance to the Information Security policy and grant exceptions (only on the genuine need basis).
3. Drafting for formulation of policy for digital payment products and services- Scope as per Annexure II
4. Review and gap assessment IT Security Policy, IT Policy, Cyber Security Policy, vendor Management Policy, BCP Policy, IS Policy etc.

Process &Timeframe

The following is an indicative timeframe for the overall selection process. Bank reserves the right to vary this timeframe at its absolute and sole discretion should the need arise. Changes to the timeframe will be relayed to the affected Respondents during the process.

Description	Due Date
Name of Bank	**The Nainital Bank Limited**
Issue quotation Notification	06.05.2021
Last date of receiving written request for clarifications	10.05.2021
Email ID for clarifications	ciso@nainitalbank.co.in
SPOC from Bank	Sunil Kumar Lohani – AVP & CISO
SPOC Mobile No	9870398868, 9871114685
SPOC Email ID	ciso@nainitalbank.co.in
Last date for submission	12.05.2021
Mode for submission of quotation **(Without Password – Password Protected)**	**On line - Password protected**
Email ID for sharing the password protected proposal *Please do not share the password other than avp.it@nainitalbank.co.in, otherwise proposal will be rejected automatically.	**ciso@nainitalbank.co.in**
Email ID for sharing Password	**avp.it@nainitalbank.co.in**
Date and time for sharing the password	**13.05.2021 by 11AM**
1- Submission of Draft policy of Information Security Policy & exception policy 2- Drafting for formulation of policy for digital payment products and services 3- Review and gap assessment IT Security Policy, IT Policy, Cyber Security Policy, vendor Management Policy, BCP Policy, IS Policy	Within 12 days from the date of PO Within 15 days from the date of PO Within 30 days from the date of PO
Submission of Final policy	Within 7 days after final feedback received from Bank.

A- COMMERCIAL FORMAT: Annexure I

B- AUDIT SCOPE: ANNEXURE II

C- **RIGHT TO REJECT:** Bank reserves the absolute and unconditional right to reject the response to this inquiry if it is not in accordance with its requirements and no further correspondence will be entertained by the Bank in the matter. The Bank may decide not to accept any quote or may accept a quote that is not a lowest quote. The bank reserves the right to cancel the tender process at any point in time

D- **Other: Keeping** in view of COVID situation NTB will allow through On Line facilities instead of onside NTB will designate a SPOC for entire SOW who would be responsible for all interactions and coordination between vendor and Bank. Bank will share the policies after execution of NDA with successful bidder. At present bank provides following services.

- Net Banking – Yes (Domestic only)
- Debit Card – Rupay Only
- Unified Payment Interface UPI –Yes (Issuer only)
- IMPS- Yes limit 5000/day-USSD/ Based bases
- ATM- White Leve ATM
- RTGS & NEFT- Yes
- SOC – Yes
- Engagement with Payment Aggregator- Yes
- DC/DR- Managed service in third Party Data Center

- Mobile Application- Under implementation
- IMPS application- Under Implementation
- NPA automation application- Yes
- AML-Yes
- ALM- Yes
- PFMS Application- Yes
- Financial Inclusion Application- Yes
- ATM Switch- Third Party
- Credit Card- NO
- SWIFT- NO

Annexure I-Commercial

Sr. No	Description	Price (Exclusive Tax)
A	Drafting for formulation of Information Security Policy & exception Policy	
B	Drafting for formulation of policy for digital payment products and services	
C	Review and gap assessment IT Security Policy, IT Policy, Cyber Security Policy, vendor Management Policy, BCP Policy, IS Policy etc.	
Total Prices includes Travelling, Lodging and other expenses		

The PO may be place to single bidder or different bidder depending upon the commercial/ bank's description.

ANNEXURE II

A- Scope: Information Security Policy: Annexure1

1- Banks need to frame Information Security Policy and identify and implement appropriate information security management measures/practices keeping in view their business needs.

2- The policies need to be supported with relevant standards, guidelines and procedures. A policy framework would, inter-alia, incorporate/take into consideration the following:

   a. An information security strategy that is aligned with business objectives and the legal requirements
   b. Objectives, scope, ownership and responsibility for the policy
   c. Information security organizational structure
   d. Information security roles and responsibilities that may include information security-specific roles like IT security manager/officer, administrators, information security specialists and information asset-specific roles like owners, custodians, end-users
   e. Periodic reviews of the policy – at least annually and in the event of significant changes necessitating revision
   f. A periodic compliance review of the policy – about the adherence of users to information security policies and put up to the information security committee.
   g. Exceptions: An exception policy for handling instances of non-compliance with the information security policy including critical aspects like exception criteria including whether there is genuine need for exceptions, management of the exception log or register, authority to grant exemptions, expiry of exceptions and the periodicity of review of exceptions granted. Where exemptions are granted, banks need to review and assess the adequacy of compensating controls initially and on an ongoing basis. A sign -off needs to be obtained from the CISO on the exceptions
   h. Penal measures for violation of policies and the process to be followed in the event of violation
   i. Identification, authorization and granting of access to IT assets (by individuals and other IT assets)
   j. Addressing the various stages of an IT asset's life to ensure that information security requirements are considered at each stage of the lifecycle
   k. An incident monitoring and management process to address the identification and classification of incidents, reporting, escalation, preservation of evidence, the investigation process
   l. Management of technology solutions for information security like a firewall, anti-virus/anti-malware software, intrusion detection/prevention systems, cryptographic systems and monitoring/log analysis tools/techniques
   m. Management and monitoring of service providers that provides for overseeing the management of information security risks by third parties
   n. Clearly indicating acceptable usage of IT assets including application systems that define the information security responsibilities of users (staff, service providers and customers) in regard to the use of IT assets
   o. Requirements relating to recruitment and selection of qualified staff and external contractors that define the framework for vetting and monitoring of personnel, taking into account the information security risk
   p. Strategy for periodic training and enhancing skills of information security personnel, requirement of continuous professional education

q. Specific policies that would be required include, but not limited to, the following:
    i. Logical Access Control
    ii. Asset Management
    iii. Network Access Control
    iv. Password management
    v. E-mail security
    vi. Remote access
    vii. Mobile computing
    viii. Network security
    ix. Application security
    x. Backup and archival
    xi. Operating system security
    xii. Database administration and security
    xiii. Physical security
    xiv. Capacity Management
    xv. Incident response and management
    xvi. Malicious software
    xvii. IT asset/media management
    xviii. Change Management
    xix. Patch Management
    xx. Internet security
    xxi. Desktop
    xxii. Encryption
    xxiii. Security of electronic delivery channels
    xxiv. Wireless security
    xxv. Application/data migration

3- Accountability for security is increased through clear job descriptions, employment agreements and policy awareness acknowledgements. It is important to communicate the general and specific security roles and responsibilities for all employees within their job descriptions. The job descriptions for security personnel should also clearly describe the systems and processes they will protect and their responsibility towards control processes. Management should expect all employees, officers and contractors/consultants to comply with security and acceptable-use policies and protect the institution’s assets, including information.

4- Given the critical role of security technologies as part of the information security framework, banks need to subject them to suitable controls across their lifecycle like guidelines on their usage, standards and procedures indicating the detailed objectives and requirements of individual information security-specific technology solutions, authorisation for individuals who would be handling the technology, addressing segregation of duties issues, appropriate configurations of the devices that provide the best possible security, regularly assessing their effectiveness and fine-tuning them accordingly, and identification of any unauthorised changes.

5- Digital evidence is similar to any other form of legal proof - it needs to withstand challenges to its integrity, its handling must be carefully tracked and documented, and it must be suitably authenticated by concerned personnel as per legal requirements. Since the evidence resides on or is generated by a digital device, a trained information security official or skilled digital forensics examiner may need to be involved in the handling process to ensure that any material facts is properly preserved and introduced. A suitable policy needs to be in place in this regard.

B- Scope of policy for digital payment products and services- Annexure2 - Please go through the RBI notification regarding “Master Direction on Digital Payment Security Controls” and cover the mentioned points in document including few of below, but not limited to, the following:

- Digital Products/Services details
- Data flow diagram mandatory for all digital payment products/services
- Secure Development life cycle for all new digital payment products
- User Acceptance Testing before introducing any new digital payment channel
- Risk Assessment for all available digital payment channel
- Third Party/Vendor guidelines and assessment for digital payment services
- Business Resilience for products and services
- Incident and Fraud Risk Management
- Change Management
- Secure Transmission and Storage of payment data
- Secure Infrastructure
- Monitoring for Mobile application and Internet banking application
- Escrow Management for application source code in case of application/product provided by third party
- Security Testing for Digital payment products
- Redact/Mask Sensitive data for SMS/Emails
- Secure Usage guidelines for customers

C- Scope of review and gap assessment IT Security Policy, IT Policy, Cyber Security Policy, vendor Management Policy, BCP Policy, IS Policy etc.

Bank already formulated and implemented Board approved policies, however keeping in view of current scenario bank want to review these polices and incorporate the identified gaps in policies. Bank will share these policies with success bidder after execution of NDA.