Expression Of Interest

A. Background of Municipal Cooperative Bank Ltd, Mumbai {MCB}.

The Bank Registered under Maharashtra Co - Operative Societies Act and has 22 Branches in City of Mumbai with Deposit base of 3226.02 Crores and Advances of 2341.53 Crores as of 31st March 2018. Bank is member of National payment Corporation of India and has issued approx. 85,000 Debit Cards to its Customers. Bank is live on ATM, POS and ECOM products of NPCI.

Bank's IT Details: Bank is on ASP with Cedge Technologies for Core banking solution which is a ISO 9001 certified company. Bank has outsourced the CBS Data with Cedge Technologies along with ATM switch and Card & pin management.

Bank offers IMPS, RTGS/NEFT, NACH, Mobile Banking and CTS services to customers

Bank is direct member of NPCI's Rupay card. Bank has enabled ATM, POS and E-Commerce facility with Rupay ATM Card.

Bank is having MTNL MPLS connectivity for all our branches with backup connectivity provided by our CBS vendor. Bank has firewall in placed at our head office from where all the links are routed to DC.

Bank is having the Information System Security Policy where in IT strategy policy is included.

B. Purpose of EOI

The Municipal Cooperative Bank Limited, Mumbai, intends to avail coverage to handle risk emanating from Crime Committed using and/or the Internet. It needs a cover against act wherein a Computer is either a tool or a target or both. Cover for acts that are punishable by the information technology Act.

To cover the above mentioned risk, we are looking to procure suitable **Cyber Liability Insurance Policy** from eligible insurance companies as per decided criteria.

C. Eligibility

General Insurance Companies satisfying the minimum eligibility criteria indicated in Annexure-I, are required to furnish their offers in the prescribed formats in Annexure-II (questionnaire on eligibility criteria and other details).

D. Scope of cover

A. Property and Theft:

1. Destruction of software system and network
2. Unrecoverable Loss of information of organisation's stored data
3. Recovery from malware or other malicious codes
4. Business interruption due to cyber-incident (Loss of net profit as a result of a material interruption to the insured's network)
5. Denial of Service
6. Information Theft – Loss of control of customer's data/record
7. Breach of intellectual property
8. Cyber Extortion and Cyber espionage
9. Losses due to cyber-terrorist acts

10. Harm to electronic media or data contents
11. Terrorism/War exclusion with carve back for Cyber terrorism
12. Social Media information, Social media banking
13. In case of Bank account information loss, credit monitoring expenses for all the lost accounts that are incurred and can extend for multiple years
14. At the time of loss of account information, certain 'Crisis Management' expenses are incurred, including PR, Call Center, Credit/Debit card, POS, other handheld devices. Replacement expenses, customer notification, etc. to protect bank's as well as customer's reputation.
15. DDoS attack on bank's network, leading to non-availability of bank's services to its customers
16. Virus, Worm, Phishing, Keylogger, Spoofing, Trojan, Bots, Spyware, Malware attacks causing downtime of critical apps viz CBS, ATM. Mobile Banking, RTGS\NEFT Interface, UPI etc.
17. Outside malicious attack (NOT technical failure) on important WAN devices of bank such as Firewall, Routers, causing application non-availability
18. Cyber Attacks
19. All Delivery channels should be covered like ATM, Internet Banking, UPI (Unified Payment Interface), Mobile banking, Mobile Wallet and other payment applications like POS etc.

B. Liability:

1)Network Security
2)Private confidentiality breach/Data Liability
   a. Loss of personal information
   b. Loss of corporate information
   c. Outsourcing
3)Reputational damage
4)Repair of the organization’s & individual’s reputation
5)Notification and Monitoring
6)Business continuity/supply chain disruptions
7)Crisis Management and response to data theft (includes costs of administrative expenses i.e. forensic investigations, penalties, regulatory and governmental fines)
8)Penalties on Bank by regulatory Authority related to Cyber Fraud case
9)Cost of repairing, replacing and updating computer systems
10) Loss of payment cards information by 3rd party service provider, leading to loss to 3rd party

C. Situation Specific Liability:

1) System Issue due to which customers could view account details of other customers through Internet banking
2) Defamatory content posted in the bank’s Mobile App by exploring weakness in the application
3) Email id of Bank’s customer hacked – Fund Transfer request received and processed by the bank – disowned by the customer
4) Card Fraud - Active (but not issued) unused Card numbers from BIN range misused to carry out fraudulent transactions
5) Data Leakage by a resigned, retired or Serving Employees
6) Data Breach – data breach due to not making a Security fix
7) Ransom threat received by bank for potential takedown of bank’s System
8) Forensic expenses to find out & fix the loopholes in the IT systems after a real or suspected cyber attack
9) Extortion money demands by cyber criminals in possession of critical data, or having a handle on important internal IT apps, capable of bringing down the IT infrastructure

10) Alteration, Damage, Deletion or destruction of data owned by the bank or for which bank is legally liable. Cost arising out of blank media, increased labor
11) DDoS attack on bank's network, leading to non-availability of bank's services to its customers causing loss of profit
12) Outside malicious attack (NOT technical failure) on important WAN devices of bank such as Firewall, Routers, causing application non-availability, causing loss of profit
13) Outside malicious attack (NOT technical failure) on important WAN devices of bank such as Firewall, Routers, causing application non-availability, causing loss of profit
14) Service provider network downtime, causing application non-availability, causing loss of profit
15) Bank employee acting on legitimate looking transaction instructions from customer, and transferring money to fraudster's account. Phishing / 'Fake President' frauds
16) Customer transferring money based on legitimate looking communication from the Bank. Subsequent loss to the customer & Bank
17) Malicious code/virus inserted by hacker, in bank's systems/software, triggering automatic money transfer from branch account (or any other account) to hacker's account
18) Mobile app based frauds, involving cloning of SIM cards to access user identity & OTP, to siphon out money from e-wallet, bank account, etc.
19) Money transferred from an account by the customer to a recipient, but NOT debited in sender's account - Using malicious code to make the software misbehave
20) Virus in the bank network making the ATM machines spew of cash
21) Loss of Payment Card information by 3rd Part service provider leading to loss to Bank or customer

Cyber Attacks May cover as:

- Backdoor
- Denial of Service Attack
- Direct Access attack
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Social Engineering Attack
- Malware
- Adware
- Bots
- Ransomware
- Rootkits
- Spyware
- Scareware
- Trojan Horses
- Bluesnarfing
- Blue jacking

E. Sum Insured / Indemnity Limit

Limit of Liability require – Option -1 10 Crores INR
Option 2 5 Crores INR

F. Participation

Required annexures as above shall be placed in an envelope duly sealed and superscribed accordingly. The envelope shall be addressed to "The General Manager (i/c), The Municipal Co – Op. Bank Ltd., Mumbai and to be delivered to Municipal Bank Bhavan, 245 – P. Dmello Road, Fort, Mumbai – 400 001. It needs to be super scribed "Expression of Interest for **Cyber Liability Insurance Policy**".

The offers should reach the above address latest by 09/10/2018 up to 5.00 PM

The offers shall be opened on the same day i.e. on 09/10/2018 in the presence of relevant council / committee members of the Bank.

General Manager(I/c)

The Municipal Co – Op. Bank Ltd., Mumbai
Municipal Bank Bhavan,
245 – P. D'mello Road,
Fort,
Mumbai – 400 001

ANNEXURE – I

Minimum Eligibility Criteria

The Insurance firm participating in the enquiry should satisfy minimum qualification criteria as under.

- Minimum 5 years' in operation as on 31St March 2017
- Minimum Solvency margin of 1.5
- Minimum gross premium underwritten – INR 2000 Crore (FY 2016-2017)
- Minimum Cyber Liability Gross Premium Underwritten – INR 20 Crores (FY 2016-2017)
- Technical underwriting team in place
- Should have handled/placed Cyber liability insurance for banks
- Should have presence in more than 10 Cities in India
- Limit of Indemnity underwritten for Cyber Liability should be at least 25 Crore

Annexure II – Questionnaire on Eligibility Criteria and other details

Sr. No.	Particulars	Response
1	Name of the Insurance Company	
2	Division Office Name & Number	
3	Division Office Address	
4	Contact Person's Name & Designation	
5	Year of Incorporation of Company	
6	Total Experience in Handling Cyber Insurance	
7	Total Amount of Premium of Cyber Liability Insurance 2016-2017	
8	Total Number of Cyber Liability Insurance Policy Issued 2016-2017	
9	Total Premium of Cyber Liability Insurance Policy 2016-2017	
10	Solvency Ratio as on 2016-2017	