Expression of Interest for Cyber Liability Insurance Policy

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

The Bank Registered under Maharashtra Co - Operative Societies Act and has 21 Branches in City of Mumbai with Deposit base of Rs. 4384 Crores and Advances of Rs. 3123 Crores as of 31st March 2025. Bank is member of National payment Corporation of India and has issued approx. One Lakh ten thousand Debit Cards to its Customers. Bank is live on ATM, POS, ECOM, IMPS and UPT products of NPCI.

From Year 2018 onwards Banks is having cyber liability insurance policy which is due for expiry on dated 24th October 2025.

Bank's IT Details: Bank is using license base software for Core Banking Solution of M/S.Finacus Solution Pvt Ltd along with the ATM switch and card & pin management. Bank has hosted its Data Center (DC) at Yotta data center Panvel NM1 which is a Tier IV Data center with hosted services and DR is located at Yotta Noida D1.

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, E-Commerce, IMPS and UPI facility with Rupay ATM Card.

Bank is having primary & secondary connectivity with latest SD-WAN technology by M/s Bharati Airtel for DC, DR all our branches. Bank has firewall in placed at our head office from where all the links are routed to DC & DR.

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 cover for losses and liabilities arising out of cyber incidents including cover for acts that are punishable by the information technology Act 2000 and The Digital Personal Data Protection (DPDP) Act 2023 and any amendments thereto.

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 acts

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, IMPS, Mobile Wallet and other payment applications like POS, Ecom etc.

20. Information & Communication asset rectification cost

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) Conduit liability

7) Fraudulent Fund Transfer

8) Social Engineering Fraud

9) Crisis Management Expenses

10) PCI DSS cover

11) Impaired access liability

12) Regulatory fines and penalties

13) Credit Monitoring

14) Business continuity/supply chain disruptions

15) Crisis Management and response to data theft (includes costs of administrative expenses i.e. forensic investigations, system clean-up cost, legal advice and representation, penalties, regulatory and governmental fines)

16) Penalties on Bank by regulatory Authority related to Cyber Fraud case

17) Cost of repairing, replacing and updating computer systems

18) Loss of payment cards information by 3rd party service provider, leading to loss to 3rd party

19) Criminal Reward Fund

20) Pro-active Forensics

21) MultiMedia Liability

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 labour

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

22) Extra Expenses cover

23) Court attendance cost

D. Other covers & clauses

1) Extended Reporting Period of 90 days

2) Emergency Costs

3) Computer system definition to include third party service providers

4) Insurer's consent is waived off for defence costs incurred for Multimedia Liability

5) Insured's consent Amended to include if mutually agreed counsel advises that there is a reasonable chance of successfully defending or reducing damages below a proposed settlement, the Insurer will pay the settlement amount it could have offered, along with the Defence Costs incurred up to that proposal. Additionally, the Insurer will cover 50% of the Loss and Defence Costs incurred after the refusal, with prior written consent.

6) Waiver of Subrogation to include if the Insured agrees in a contract to waive the Insurer's subrogation rights against another party, and the agreement is made before any wrongful act by that party, the Insurer's subrogation rights will be waived.

7) Control Group Clause

8) Non Cancellation Clause: Policy may not be cancelled except for non-payment of premium by the Policyholder.

9) Unauthorized or unlawfully collected data Exclusion deleted

10) Intentional acts Exclusion deleted

11) Data risk Exclusion Deleted

12) Unsolicited materials Exclusion Deleted

13) Criminal acts Exclusion Deleted

14) Conduct Exclusion Deleted

15) Cover for New Subsidiary

16) Psychological Support Expenses

Cyber Attacks May cover as:

1. Backdoor
2. Denial of Service Attack
3. Direct Access attack
4. Spoofing
5. Tampering
6. Repudiation
7. Information Disclosure

8. Social Engineering Attack
9. Malware
10. Adware
11. Bots
12. Ransomware
13. Rootkits
14. Spyware
15. Scareware
16. Trojan Horses
17. Bluesnarfing
18. Blue jacking

E. Sum Insured / Indemnity Limit

Limit of Liability require –15 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, 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 **15/10/2025 upto 5.00 PM**

General Manager

The Municipal Co – Op. Bank Ltd., Mumbai

Municipal Bank Bhavan,

245 – P. D'mello Road,

Fort, Mumbai – 400 001

Email: mcb.itcell@mcbmumbai.com

Contact: 022-22717858/52

ANNEXURE – I

Minimum Eligibility Criteria

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

1. Minimum 5 years' in operation as on 31st March 2025
2. Minimum Solvency margin of 1.5
3. Minimum gross premium underwritten – INR 2000 Crore (in each of the last 3 FYs)
4. Minimum Cyber Liability Gross Premium Underwritten – INR 20 Crores (in each of the last 3 FYs)
5. Technical underwriting team in place
6. Should have handled/placed Cyber liability insurance for Banks
7. Should have presence in more than 10 Cities in India
8. Limit of Indemnity underwritten for Cyber Liability should be at least 25 Crore (in each of the last 3 FYs)

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 in last 3 FYs (Specify separately for Banks and other insureds)	
8	Total Number of Cyber Liability Insurance Policy Issued in last 3 FYs (Specify separately for Banks and other insureds)	
9	Total Number of Cyber Liability Insurance Claims Settled in last 3 FYs	
10	Total claims amount for Cyber Liability Insurance Claims Settled in last 3 FYs	
10	Solvency Ratio as on 31st March 2025	