

## Request for Proposal (RFP) for Renewal of Cyber Risk Insurance Policy for the Bank of Maharashtra

### Tender Notice

Bank of Maharashtra invites sealed offers from Public sector General insurers for procurement of Cyber Risk Insurance Policy for the bank. Please visit our website [www.bankofmaharashtra.in](http://www.bankofmaharashtra.in) for the notice of the tender.

The detailed RFP can be requested for from the below email Id's:

[trupti.alti@mahabank.co.in](mailto:trupti.alti@mahabank.co.in)

[cmcs@mahabank.co.in](mailto:cmcs@mahabank.co.in)

Addendum / Corrigendum, if any, to this tender will be published only on Bank's website.

Date of commencement of issue of RFP	: 4 <sup>th</sup> November 2019
Last date for receipt of RFP queries	: 13 <sup>th</sup> November 2019 upto 4.00 pm.
Last date of receipt of RFP responses	: 14 <sup>th</sup> November 2019
Last date for submission of RFP by bidders	: 16 <sup>th</sup> November 2019 upto 3.00 pm

Bank of Maharashtra,  
Central Office, Lokmangal, 1501, Shivajinagar Pune- 411005.

## **DISCLAIMER**

The information contained in this Request for Proposal (RFP) is provided to the Bidder(s) on the terms and conditions set out in this RFP document. The RFP document contains statements derived from information that is believed to be true and reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Bank in relation to the provision of services. The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the Bank and any successful Bidder as identified by the Bank, after completion of the selection process as detailed in this document. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officers of Bank of Maharashtra with the Bidder. The purpose of this RFP is to provide the Bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct their own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Bank of Maharashtra makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Bank of Maharashtra may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

## Schedule of Events and Bid Details

Date of issue of RFP	4 <sup>th</sup> November 2019
Last date and time for submission of query	13 <sup>th</sup> November 2019 upto 4.00 pm.
Bid related queries Response	14 <sup>th</sup> November 2019.
Address for communication and contact number	Bank of Maharashtra, Head Office, Lokmangal, 1501, Shivajinagar Pune-411005. Contact No –( 020) 25614367,25614331.
Last date for submission Of Bidding Document	16 <sup>th</sup> November 2019 at 3:00 pm
Date and Time of Technical Bid Opening	16 <sup>th</sup> November 2019 at 4:00 pm
Place of Opening of Bids	Bank of Maharashtra, Corporate Services Department, Head Office, Lokmangal, 1501, Shivajinagar Pune-411005.

Note: Any bid received after target date of the receipt of bids prescribed as mentioned above, will not be accepted by the Bank. Bids once submitted will be treated as final and no further correspondence will be entertained on this. No bid will be modified after submission of bids. No bidder shall be allowed to withdraw the bid.

## Table of Contents

<b>Sr. No</b>	<b>Contents</b>	<b>Page No.</b>
1	Introduction	6
2	Objectives of the RFP	6
3	Eligibility Criteria	6
4	Scope of Work	6
5	Proposal Process Management	8
6	Language of Bid	8
7	Technical Bid	8
8	Commercial Bid	8
9	Summary of Proposal Format	9
10	Payment Terms	9
11	Overview of Evaluation Process	9
12	Proposal ownership	9
13	Bidder's Liability	10
14	Rejections of Bids	10
15	Modifications and/or Withdrawal of Bid	10
16	Price	10
17	Notification of Award	10
18	Purchase Order	10
19	Bid Validity	10
20	Amendments to Bidding Documents	11
21	No Commitment to Accept Lowest or Any Tender	11
22	Governing Law and Disputes	11
23	Confidentiality	11
24	Resolutions of Disputes	11
25	Clarifications	12
26	Arbitrations	12
27	Jurisdictions	12
28	Submission of bids	12

29	Annexure A – Technical Bid	
	Part I: Eligibility Criteria	13
	Part II: quote slip and draft policy wording	14 & 15-48
30	Annexure B – Commercial Bid Format	49
31	Annexure C – Bid Query Format	50
32	Annexure D – Covering Letter (to the Bank on the bidder’s letterhead)	51
33	Annexure E – Undertaking by Bidder	52

## **1 Introduction**

**Bank of Maharashtra** , (hereinafter called as “**Bank**” or “**the Bank**”) a Public Sector Bank has its Head Office at 1501, Lokmangal, Shivajinagar, Pune- 411005. The bank has 15 million customers across the length and breadth of the country served through 1832 branches as of 3009.2019. It has largest network of branches by any public sector bank in the state of Maharashtra.

## **2 Objectives of the RFP**

- 2.1 Bank intends to procure a Cyber Risk Insurance Policy for sum insured values along with list of coverages as stated in section 4 of this document - Scope of work and the policy period being 1 year.
- 2.2 Bank of Maharashtra intends to issue this bid document, hereinafter called RFP, to eligible Insurance Service Providers in India, hereafter called as “Bidders or Vendors”, to participate in the competitive bidding for Cyber Risk Insurance Policy for the Bank for sum insured value along with list of coverages as stated in section 4 of this document - Scope of work and the policy period being 1 year.
- 2.3 All offers of the bidders shall be unconditional and once accepted whether with or without modifications by the Bank shall be binding between the Bank and such Bidder.
- 2.4 Bank will not accept any deviations from the terms and conditions specified in this RFP document. Deviations could result in disqualification of the offer made by the vendor at the discretion of the Bank.

## **3 Eligibility Criteria**

Only those bidders fulfilling these criteria should respond to the tender:

1. The bidder should have a valid insurance license to provide requisite insurance and claims settlement services in India with the requisite documentation from the regulator in that regard in their possession. The license should be valid for the policy servicing period.
2. Bidder should be a Government organization / PSU or a registered/ incorporated company in India under the Companies Act 1956 / 2013 and having business in India during last 5 years.
3. The Bidder should have market share of 1% in the general insurance industry during the last three fiscal years i.e. 2016-2017, 2017-18 and 2018-19. This must be the individual company turnover and not that of any group of companies.

Note: Bidder should submit proof in support of above mentioned criteria while submitting the proposal, the same is to be submitted as Part I of Technical Bid document as per Annexure - A. Vendors who do not fulfill the above criteria or who fail to submit proof will be rejected ab initio.

## **4 Scope of Work**

Bank intends to procure a Cyber Risk Insurance Policy for sum insured values and list of coverages as

stated in Clause No. 4.1 below and Annexure A.

**4.1 The following terms and conditions of the quote slip (to be adhered to) without any Deviation and form the basis upon which the Technical Bid is to be provided:**

Policy Type	Cyber Risk Insurance Policy
Named Insured	Bank of Maharashtra
Territory & Jurisdiction	Worldwide
Communication Address	Bank of Maharashtra 1501, Lokmangal, Shivajinagar, Pune- 411005
Period of Insurance	26 <sup>th</sup> November 2019 to 25 <sup>th</sup> November 2020
Retroactive Date	26 <sup>th</sup> September 2017
Business Description	Banking and Financial Services
Currency of Quote	Rs.75 Crores
Indemnity Limit	Rs. 75 Crores
Deductible	Option 1: Rs 25 Lakhs Option 2: Rs 15 Lakhs
Coverages	
1.	Data Liability
2.	Administrative Obligations
3.	Reputation & Response Cost
4.	Multimedia Liability
5.	Cyber / Privacy Extortion
6.	Network Interruption
7.	PCI DSS Assessment
8.	Reward Expenses
9.	Fraudulent Communication Loss
10.	Cyber Terrorism
11.	Psychological Support Expenses
12.	Fraudulent Fund Transfer Loss
13.	Social Engineering Fraud

**“This tender document is not transferable. Only the bidder, who purchased this tender is entitled to quote ”**

**The Policy wordings for all the above coverages is attached as per Part II of the Technical bid- Annexure A and the same needs to be submitted and agreed upon in toto by the participating bidders**

## **5 Proposal Process Management**

- 5.1 Bank of Maharashtra reserves the right to accept or reject any or all proposals, to revise the RFP, to request one or more re- submissions from all bidders or clarifications from one or more bidders, or to cancel the process in part or whole. All claims for functional/technical delivery made by the bidders in their responses to the RFP shall be assumed as deliverable within the quoted financials.
- 5.2 The Bidder shall bear all costs associated with the preparation and submission of its bid, and the Bank will, in no case be responsible or liable for those costs.

## **6 Language of Bid**

The language of the bid response and any communication with the Bank must be written in English only. Supporting documents provided with the RFP response can be in another language so long as it is accompanied by an attested translation in English, in which case, for purpose of evaluation of the bids, the English translation will govern.

## **7 Technical Bid:**

- 7.1 **The Technical Bid** - Part I and Part II of annexure A should be complete in all respects and contain all information asked for in these documents. It should not contain any price information.
- 7.2 The following original documents in physical form are to be submitted to the bank :
  - 7.2.1 Eligibility criteria as provided for in (Part I) of Annexure A, along with supporting documents attached
  - 7.2.2 The quote slip and draft policy wordings as provided for in (Part II) of Annexure A to be submitted without deviation in any terms and deviated terms if any will be discarded as ab- initio.
  - 7.2.3 Annexure D & Annexure E are to be submitted in this envelope as per format prescribed by the Bank and should bear the bidders' seal and the name, designation and signature of the Authorised Signatory of the bidder.
- 7.3 The bidder should ensure that all the annexures are submitted as prescribed by the Bank. In case it is not in the prescribed format, it is liable to be rejected.
- 7.4 The Bank further reserves the right to reject any or all offers based on its own evaluation of the offers received, or based on stability, capabilities, track records, reputation among users and other similar features of a bidder.
- 7.5 The Bank reserves the right to modify any terms, conditions or specifications for submission of bids and to obtain revised Bids from the bidders due to such changes, if any at any time prior to completion of evaluation of technical bids from the participating bidders.

In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank, at its discretion, may extend the deadline for a reasonable period as decided by the Bank for the submission of Bids.

## **8 Commercial Bid**

- 8.1 The Commercial bid must be submitted as provided for in the template attached as Annexure B
- 8.2 Opening of the commercial bids will be subject to the vendors getting shortlisted on the basis of technical evaluation.



## 9 Summary of Proposal Format

The RFP should be submitted in two separate sealed envelopes:

**Sealed Envelope 1** – All the below annexures to be submitted:

- Technical Bid – Annexure A (Part I – Documents pertaining to Eligibility criteria)
- Technical Bid – Annexure A (Part II – Quote Slip + Draft Policy wordings)
- Annexure D & Annexure E

Envelope containing the above annexures should have the name of the bidder mentioned on the envelope and titled as – **“Technical bid for Cyber Risk Insurance Policy for the Bank”**

**Sealed Envelope 2** – Annexure B to be submitted in this envelope

Envelope containing the above annexure should have the name of the bidder mentioned on the envelope and titled as – **“Commercial bid for Cyber Risk Insurance Policy for the Bank”**

## 10 Payment Terms

- 10.1 Premium will be paid as per IRDA guidelines
- 10.2 All the payments will be made to bidder electronically in Indian Rupees only
- 10.3 Bank will pay the policy premium as per the invoice raised before policy inception

## 11 Overview of Evaluation Process

- 11.1 Technical and Commercial Bid to be submitted by bidder as per stipulated date/time, address and the manner as mentioned above in this document
- 11.2 The bidders to appoint one representative to act as executive representative of the bidder for all future correspondence, bidder to provide contact details of such a representative.
- 11.3 The bids will be opened as per tender schedule as mentioned above, at location of the bank and the same will be opened in front of the respective executive representatives of the bidders.
- 11.4 In the event of the specified date of bid opening being declared a holiday for the Bank, the bids shall be opened at the appointed time and place on next working day.
- 11.5 Contingent to the validation of the eligibility criteria being met, the bidder’s official submission will be taken into consideration. With immediate disqualification in case of any discrepancy in that regard.
- 11.6 The first bid to be evaluated would be that of the “Technical Bid”
- 11.7 The bidder who agrees to all the terms and conditions of the technical bid and is L1 in the financial bid will be awarded this tender
- 11.8 The L1 winning bidder shall proceed with due process to commence procurement of the Cyber Risk Insurance policy and the requisite servicing.

## 12 Proposal Ownership

The proposal and all supporting documentation submitted by the vendors shall become the property of Bank of Maharashtra unless the bank agrees to the vendor’s specific requests, in writing, that the proposal and documentation be returned or destroyed.

### **13 Bidder's Liability**

The Bidder's liability in case of claims against the Bank resulting from gross misconduct or gross negligence of the Bidder, its employees, contractors, and subcontractors or from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.

### **14 Rejection of Bids**

- 14.1 The document does not bear signature of authorized person in each page and duly stamped.
- 14.2 It is received through Fax/E-mail.
- 14.3 It is received after expiry of the due date stipulated for Bid submission.
- 14.4 It is Incomplete including non-submission or non-furnishing of requisite documents / Conditional Bids / Bids not conforming to the terms and conditions stipulated in this Request for proposal (RFP)
- 14.5 It is evasive or contains incorrect information
- 14.6 Any form of canvassing / lobbying /influence/ query regarding short listing, status etc. is made.
- 14.7 It does not comply with all the points mentioned in the scope of work. Noncompliance of any RFP clause will lead to rejection of the bid.
- 14.8 Bids not containing an Undertaking (as per Annexure E) to the Bank, on their letter head.

### **15 Modifications and/or Withdrawal of Bid**

- 15.1 No bid will be allowed to be submitted or modified after the deadline for submission of bids.
- 15.2 No bid shall be withdrawn in the intervening period between deadlines for submission of bids.
- 15.3 No bidder shall be allowed to withdraw the bid, if bidder happens to be successful bidder.

### **16 Price**

There shall be no increase in premium for any reason whatsoever during the policy period. Any standard clauses in the policy document pertaining to increase of premium or modification or alteration of RFP terms and conditions shall not be accepted during the policy period

### **17 Notification of Award**

After selection of the L1 bidder and after obtaining internal approvals and prior to expiration of the period of Bid validity, the Bank will send Notification of Award /Purchase Order to the selected Bidder

### **18 Purchase Order**

- 18.1 Within 15 working days of receipt of Notification of Award, the successful Bidder shall accept the Purchase Order and issue the policy document to the bank.
- 18.2 Failure of the successful Bidder to comply with the above requirements shall constitute sufficient grounds for the annulment of the award.

### **19 Bid Validity**

The bidder shall keep the bid valid for 60 days from the last date of submission of bids.

## **20 Amendments to Bidding Documents**

- 20.1 Bank reserves the right to alter the RFP terms and conditions at any time before submission of the bids.
- 20.2 Prior to the last date for bid-submission, the Bank may, for any reason, whether at its own initiative or in response to clarification(s) sought from the prospective Bidders, modify the RFP contents/ covenants by amendment and the same will be published as an addendum/Corrigendum on the bank's website and government portal

## **21 No Commitment to Accept Lowest or Any Tender**

- 21.1 The Bank shall be under no obligation to accept the lowest or any other offer received in response to this tender notice.
- 21.2 The Bank further reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar credentials of a vendor. When the Bank makes any such rejection, the Bank will not be bound to give any reason and/or justification in this regard to the vendor.

## **22 Governing Law and Disputes**

The Bid and the subsequent Contract with the selected Bidder shall be governed in accordance with the Laws of India and will be subject to the exclusive jurisdiction of Courts in Pune.

## **23 Confidentiality**

- 23.1 This document contains information confidential and proprietary to the Bank. Disclosures of receipt of this RFP or any part of the aforementioned information to parties not directly involved in providing the services requested could result in the disqualification of the vendors, premature termination of the contract, and / or legal action against the vendors for breach of trust.
- 23.2 The vendor (and his employees) shall not, unless the Bank gives permission in writing, disclose any part or whole of this RFP document, of the proposal and/or contract, or any specification, sample or information furnished by the Bank (including the users), in connection therewith to any person other than a person employed by the bidder in the performance of the proposal and/or contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance. The employees or the third party Engaged by the bidder will maintain strict confidentiality
- 23.3 The vendor, his employees and agents shall not, without prior written consent from the Bank, make any use of any document or information given by the Bank or its Authorized personnel, except for purposes of performing the contract award.
- 23.4 In case of breach the Bank shall take such legal action as it may be advised.

## **24 Resolutions of Disputes**

- 24.1 All disputes and differences of any kind, whatsoever, between the Supplier and the Bank, arising out of or in relation to the construction, meaning, operation or effect of the Contract, shall be settled amicably by both Bank and the vendor. If after thirty days from the commencement of such informal negotiations, Bank and the vendor are unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution by formal arbitration.

24.2 All questions, disputes or differences arising under and out of, or in connection with the RFP, shall be referred to a panel of three Arbitrators: one Arbitrator to be nominated by the Bank and the other to be nominated by the vendor. Two Arbitrators so appointed shall appoint the third Arbitrator. The award of the Arbitrator shall be final and binding on the parties. The Arbitration and conciliation act 1996 or any statutory modification or reenactment thereof for the time being enforced, shall apply to the arbitration proceedings and the venue and jurisdiction for arbitration shall be at Pune, India. In case the vendor would like to exit the project, the same shall be taken up by the Arbitration process.

## 25 Clarifications

25.1 All queries and clarifications regarding the RFP must be sent to the below e-mail id's – [trupti.alti@mahabank.co.in](mailto:trupti.alti@mahabank.co.in) [cmcs@mahabank.co.in](mailto:cmcs@mahabank.co.in) with subject "RFP Clarifications – for Procurement of Cyber Risk Insurance Policy of the Bank" as per the date given in the schedule of events of this RFP document.

## 26 Arbitrations

All disputes and differences of any kind whatsoever arising out of or in connection with the purchase order shall be referred to arbitration. The arbitrator may be appointed by both the parties or in case of disagreement each party may appoint an arbitrator and such arbitrators shall appoint an Umpire before entering on the reference. The decision of the Umpire shall be final. Such arbitration shall be governed by the provisions of The Arbitration and Conciliation Act 1996. All arbitration proceedings shall be at Pune.

"Language of the arbitration proceeds be in English."

## 27 Jurisdictions

Notwithstanding anything contained herein above, in case of any dispute, claim and legal action arising out of this RFP, the parties shall be subject to the jurisdiction of courts at Pune.

## 28 Submissions of Bids

The bidders have to submit bids physically in sealed cover at the following address on or before 16<sup>th</sup> November 2019 upto 3.00 pm.

To,  
The Asst.General Manager,  
Corporate Services Dept.  
Bank of Maharashtra,  
Head Office,  
1501, Lokmangal,  
Shivajinagar, Pune-411005.

## 29 Annexure A – Technical Bid

### Part I: Eligibility Criteria

Eligibility Criteria for Bidder	Supporting Documents Required	Complied (Yes/No)
Bidder should have a valid insurance license to provide requisite insurance and claims settlement services in India with the requisite documentation from the regulator in that regard in their possession. The license should be valid for the policy servicing period.	Copy of license issued by IRDAI to be submitted	
Bidder should be a Government organization / PSU or a registered/ incorporated company in India under the Companies Act 1956 /2013 and having business in India during last 5years	copy of certificate of incorporation to be submitted	
The Bidder should have market share of 1% in the general insurance industry during the last three fiscal years i.e. 2016-17, 2017-2018 and 2018-19. This must be the individual company turnover and not that of any group of companies	Audited Financial Statements for the financial years 2016-17, 2017-18 and 2018-19 to be submitted  OR  Certified letter from the Chartered Account. The CA certificate in this regard should be without any riders or qualification.	

### Authorized Signatory

(Name, Designation and Seal of the Company)

Date:

**DRAFT POLICY WORDINGS**

**Cyber Risk Insurance Policy**

**For**

**Bank of Maharashtra**

**POLICY NUMBER-**

**Period of Insurance**

**26<sup>th</sup> November 2019 to 25<sup>th</sup> November 2020**

## Schedule

Policy Number:			
<b>1. Policy Holder Name:</b>	<b>Bank of Maharashtra</b>		
<b>2. Policy Holder main Address</b>	Head Office, 1501, Lokmangal, Shivajinagar, Pune - 411005		
<b>3. Inception Date</b>	<b>(DD/MM/YYYY)</b>		
<b>4. Policy period</b>	<b>From: (26/11/2019) To: (25/11/2020)</b>		
	Both days inclusive at the <b>Policyholder's</b> main address		
<b>5. Limit of Liability</b>	Aggregate <b>Limit of Liability</b> per <b>Policy Period</b> for all <b>Loss</b> of all <b>Insured's</b> under all insurance covers combined (A, B, C, and all <b>Extension</b> ): Rs. 75 crore		
<b>6. Coverages and Extensions</b>	<b>Data Administrative Investigations:</b>		
	<b>Data Administrative Fines:</b>		
	<b>Pro-active Forensic Services:</b>		
	<b>Repair of the Company's Reputation:</b>		
	<b>Repair of the Individual's Reputation:</b>		
	<b>Restoring, recreating, or recollecting Electronic Data:</b>		
	<b>Multimedia Liability:</b>		
	<b>Cyber/Privacy Extortion:</b>		
	<b>Network Interruption:</b>		
	<b>PCI DSS Assessment</b>		
	<b>Reward Expenses</b>		
	<b>Fraudulent Communication Loss</b>		
	<b>Cyber Terrorism</b>		
	<b>Psychological Support Expenses</b>		
	<b>Fraudulent Fund Transfer Loss</b>		
<b>Social Engineering Fraud</b>			
<b>7. Deductible</b>	<table border="1" style="width: 100%;"> <tr> <td style="width: 70%;"><b>General Policy Deductible</b></td> <td><b>Option 1 :Rs 25 Lakhs</b></td> </tr> </table>	<b>General Policy Deductible</b>	<b>Option 1 :Rs 25 Lakhs</b>
<b>General Policy Deductible</b>	<b>Option 1 :Rs 25 Lakhs</b>		

		<b>Option 2 :Rs 15 Lakhs</b>
	<b>Network Interruption</b>	<b>Waiting Hours Period: 12 hours</b>
<b>8. Annual Premium (Including GST)</b>		
<b>9. Retroactive Date</b>	<b>26<sup>th</sup> September 2017</b>	
<b>10. Insurer &amp; Address</b>		
<b>11. Claims Notice</b>		



## 1. COVERAGES

In consideration of the payment of the annual premium and subject to all of the provisions of this policy the **Insurer** and the Policyholder agree as follows:

Cover under this policy is written specifically on a primary basis and are provided solely for Claims first made against an **Insured** during the Policy Period and reported to the **Insurer** in accordance with the conditions of this policy.

It applies only to acts, errors or omissions of an **Insured** committed after the Retroactive Date.

### A. DATA LIABILITY

#### A.1 Loss of Personal Information

The **Insurer** will pay to or on behalf of any **Insured** all Damages and Defence Costs which arise out of a Claim by a Data Subject against the **Insured** in respect of an actual or alleged Qualifying Breach of Personal Information

#### A.2 Loss of Corporate Information

The **Insurer** will pay to or on behalf of any **Insured** all **Damages** and **Information Defence Costs** which arise out of a **Claim** by a **Third Party** against the **Insured** in respect of an actual or alleged **Qualifying Breach of Corporate Information**

#### A.3 Outsourcing

The **Insurer** will pay to or on behalf of any **Company** all **Damages** and **Defence Costs** which arise out of a **Claim** by a **Third Party** against an **Outsourcer** (where the **Company** has a contractual duty to indemnify) and which arises from any actual or alleged breach of duty by the **Outsourcer** in regards to the processing of **Personal Information** and/or **Corporate Information** on behalf of the **Company** (for which the **Company** is liable).

#### A.4 Network Security

The **Insurer** will pay to or on behalf of any **Insured** all **Damages** and **Defence Costs** which arise out of a **Claim** by a **Third Party** against the **Insured** which is caused by any act, error or omission by the **Insured** resulting in:

- (i) The introduction of any unauthorized software, computer code, including malicious code or virus to **Third Party Data** on the **Company's Computer System** which is specifically designed to disrupt the operation of or corrupt or damage any software or data recorded on the **Company's Computer System**;
- (ii) The denial of access to an authorized **Third Party** to its **Data**;
- (iii) The wrongful appropriation of a network access code from the **Company**;
- (iv) The destruction, modification, corruption, damage or deletion of **Third Party Data** stored on any **Computer System**;
- (v) The physical theft of the **Company's Assets** by a **Third Party**, or its physical loss; or
- (vi) The disclosure of **Third Party Data** by an employee of the **Company**

## **B. ADMINISTRATIVE OBLIGATIONS**

### **B.1 Data Administrative Investigation**

The **Insurer** will pay to or on behalf of any **Insured** all **Professional Fees** for legal advice and representation in connection with any **Regulatory Investigation**

### **B.2 Data Administrative Fines**

The **Insurer** will pay to or on behalf of any **Insured** all **Data Administrative Fines** that the **Insured** is legally obligated to pay upon the conclusion of a **Regulatory Investigation** arising out of a breach of **Data Protection Law**.

## **C. REPUTATION AND RESPONSE COSTS**

### **C.1 Pro-active Forensic Services**

The **Insurer** will pay to or on behalf of any **Company** all **Professional Fees** of forensic cyber risk specialists for the purpose of substantiating whether a **Qualifying Breach of Data Security** has occurred/is occurring, identifying the cause, establishing the extent of the breach, identify **Personal information** and **Corporate Information** that may have been compromised and for making recommendations as to how this may be prevented, mitigated or resolved. Such **Professional Fees** can only be incurred from the date of notification to the **Insurer** in accordance with clause 5.3.

### **C.2 Repair of the Company's Reputation**

The **Insurer** will pay to or on behalf of any **Company** all **Professional Fees** of independent advisors (including, but not limited to, legal advice concerning media strategy, crisis consulting and independent public relations services) for the management of any action reasonably required to prevent or mitigate the potential adverse effect of a **Newsworthy Event** including the design and management of a communications strategy.

Such **Professional Fees** can only be incurred from the date of notification to the **Insurer** in accordance with clause 5.1 to the date falling 185 days after such notification.

### **C.3 Repair of the Individual Reputation**

The **Insurer** will pay to or on behalf of any director, chief compliance officer, **Data Protection Officer** or General Counsel of a **Company** all **Professional Fees** for advice and support from an independent public relations consultant, in order to mitigate or prevent damage to their individual (personal and professional) reputation due to an actual or alleged **Qualifying Breach of Data Security** or breach of **Data Protection Law**. Such **Professional Fees** can only be incurred from the date of notification to the **Insurer** in accordance with clause 5.1 to the date falling 185 days after such notification.

### **C.4 Notification to Data Subjects**

The **Insurer** will pay to or behalf of the **Insured** all **Professional Fees**, call centre expenses and ID theft remediation expenses in relation to the investigation, collation of information,

preparation for and notification to **Data Subjects** and/or any relevant **Regulator** of any alleged or actual **Qualifying Breach of Data Security** or breach of **Data Protection Law**

### **C.5 Monitoring**

The **Insurer** will pay to or on behalf of the **Company** all **Professional Fees** for credit monitoring services and cost of customer credits for possible misuse of any Personal **Information** as a result of an actual or alleged **Qualifying Breach of Data Security** or breach of **Data Protection Law**.

### **C.6 Electronic Data**

The **Insurer** will pay to or on behalf of the **Company** all **Professional Fees** to:

- (i) determine whether **Data** held by the **Company** can or cannot be restored, recollected, or recreated; and
- (ii) Recreate or recollect **Data** held by the **Company** where backup systems fail to capture such **Data** or it is corrupted or lost because of a technical failure or because of the negligence or default of an operator or other person lawfully charged with that responsibility

## EXTENSIONS

Extensions are subject to the terms, conditions, definitions and exclusions of this policy and the additional terms, conditions, definitions and exclusions in this section.

### D. MULTIMEDIA LIABILITY

#### D.1 Multimedia Liability

In consideration of the additional premium paid, the **Insurer** will pay to or on behalf of any **Company** all **Damages** and **Defence Costs** which arise out of a **Claim** by a **Third Party** against the **Company** solely in the performance of or failure to perform **Multimedia Activities** arising from the following alleged or actual wrongful acts:

- (i) defamation, including but not limited to libel, slander, or disparagement of trade, reputation or the character of any person or organization, or infliction of emotional distress or mental anguish arising from the foregoing;
- (ii) unintentional infringement of copyright, title, slogan, trademark, trade name, trade dress, mark, service mark, service name or domain name, whether by deep-linking or framing or otherwise;
- (iii) plagiarism, piracy or misappropriation or theft of ideas or information;
- (iv) invasion, infringement or interference with rights of privacy or publicity, false light, public disclosure of private facts, intrusion and commercial appropriation of name, persona or likeness;
- (v) unfair competition, but only if alleged in conjunction with any of the acts listed in (i) – (iv) above; or
- (vi) liability arising out of the **Insured's** negligence in respect of any digital media content.
- (vii) cost of specialist stop, remove and suppress the content/ harmful articles published in internet through breaching company's official social media webpage.

#### D.2 Definitions

**Multimedia Activities** means the publication or broadcast of any digital media content and written media

#### D.3 Exclusions

##### Product Descriptions

This Extension shall not cover **Loss** arising out of, based upon or attributable to the actual or alleged inaccurate, inadequate, or incomplete description of the price of goods, products, or services and any cost guarantees, cost representations, or contract price estimates, the authenticity of any goods, products or services, or the failure of any goods or services to conform with any represented quality or performance standards

## Financial Data

This Extension shall not cover **Loss** arising out of, based upon or attributable to errors made in any financial data that the **Company** publicizes including, but not limited to, the **Company's** annual report and accounts and any communications to the stock market.

## E. CYBER/ PRIVACY EXTORTION

### E.1 Cyber/Privacy Extortion Liability

In consideration of the additional premium paid, the **Insurer** will pay to or on behalf of the **Insured** all **Extortion Loss** that an **Insured** incurs solely as a result of an **Extortion Threat**.

### E.2 Definitions

**Extortion Loss** Means any:

- I. Monies paid by an **Insured** with the **Insurer's** prior written consent to prevent or end an **Extortion Threat**; or
- II. **Professional Fees** for independent advisors to conduct an investigation to determine the cause of and to end an **Extortion Threat**.
- III. **Ransom** money lost in transit.

**Extortion Threat** Means any threat or connected series of threats, for the purpose of demanding monies, communicated to the **Insured** to prevent or end a **Security Threat**

**Security Threat** Means any threat to the **Computer System** that may result in an actual or alleged **Qualifying Breach of Data Security** causing financial harm to the **Company**.

### Conditions

The **Policyholder** and the **Insured** will use all reasonable efforts not to disclose the existence of this Policy

The **Insured** shall allow the **Insurer** (or the **Insurer's** nominated representatives) to notify the police or other responsible law enforcement authorities of any **Extortion Threat**

## F. NETWORK INTERRUPTION INCLUDING SYSTEM FAILURE COVERAGE

### F.1 Network Interruption Insurance

In consideration of the premium paid, the **Insurer** will pay to the **Company** any **Network Loss** in respect of a **Material interruption** that an **Insured** incurs after the **Waiting Hours Period** has expired and solely as a result of a **Security Failure** or **System Failure**

### F.2 Definitions

**Material Interruption** means any material interruption in, or suspension of, the service provided by the **Computer System** directly caused by a **Security Failure** or **System Failure**

**Network Loss** means the reduction in net profit earned by the **Company** in the period from the expiration of the **Waiting Hours Period** until service is restored (but in any event no later than 90 days after the commencement of the **Material Interruption**) that, but for the **Material Interruption**, the **Company** would have earned (and which is attributable to a loss of revenue) before payment of income taxes and after accounting for savings and reasonable mitigation.

**Network Loss** includes continuing normal operating expenses incurred (including payroll) and additional expenditure incurred for the purpose of minimizing the **Material Interruption**; provided, however, that in the case of **System Failure** such sum shall not exceed the **System Failure Hourly Percentage** of the **System Failure Sublimit** if any during any one hour period and any amount in excess of the **System Failure Hourly Percentage** of the **System Failure Sublimit** during any one hour period shall not be **Network Loss**.

**Network Loss** shall be reduced by any amounts recovered by an **Insured** (including, without limitation, the value of any service credits provided to an **Insured**) from any third party (including, without limitation, any **Outsource Service Provider**) in connection with or as a result of a **System Failure** or **Security Failure**.

**Network Loss** excludes losses arising from **Claims** made by **Third Parties** for whatever reason but not a reduction in revenue by virtue of a contractual reduction in payments for the service or service credits paid by the **Insured**

**Security Failure** Means a failure or intrusion of the **Computer System**, including, without limitation, that which results in or fails to mitigate any damage, corruption or deletion of data unauthorized access, unauthorized use, denial of service attack or receipt or transmission of a malicious code. **Security Failure** includes any such failure or intrusion resulting from the theft of a password or network access code from a **Company's** premises, a **Computer System**, or an officer, director or employee of a **Company** by non- electronic means in direct violation of a **Company's** specific written security policies or procedures.

**System Failure** means any unintentional and unplanned outage of a **Computer System**.

**Outsource Service Provider** means an entity not owned, operated or controlled by an **Insured** that such **Insured** depends on to conduct its business

**Waiting Hours Period** Means the number of hours set forth in item 7 of the Schedule that must elapse once a **Material Interruption** has begun before a **Network Loss** can begin to be incurred.

### **F.3 Exclusions**

#### **Government Entity or Public Authority**

This Extension shall not cover any **Network Loss** arising out of, based upon or attributable to any seizure, confiscation, nationalization, or destruction of a **Computer System** by order of any government entity or public authority

### Specific Network Interruption Conditions

This Extension shall not cover any **Network Loss** arising out of, based upon or attributable to any:

- I. Network or systems interruption caused by loss of communications with a **Third Party** computer system, resulting in the inability of the **Company** to communicate with those systems;
- II. Legal costs or legal expenses of any type; or
- III. Unfavorable business conditions.

### F.4 Notice

In addition to the requirements to give notice under this policy, and before coverage will apply, each **Insured** must also:

- (i) complete and sign a written, detailed and affirmed proof of loss within ninety (90) days after the discovery of any **Network Loss** (unless this period is otherwise extended in writing by the **Insurer**) which will detail a full description of the **Network Loss** and the circumstances of such **Network Loss**. The written proof should also include a detailed calculation of any **Network Loss** and all underlying documents and materials that reasonably relate to or form a part of the basis of the proof of the Network Loss;
- (ii) Upon the **Insurer's** request, submit to an examination; and
- (iii) Waive professional privilege and shall provide the **Insurer** on an ongoing basis with any cooperation and assistance that the **Insurer** may request, including assisting the **Insurer** in:
  - a) any investigation of a **Security Failure** or **Network Loss**;
  - b) enforcing any legal rights the **Company** or the **Insurer** may have against anyone who may be liable to an **Insured** for a **Security Failure**;
  - c) executing any documents that the **Insurer** deems necessary to secure its rights under this policy; and
  - d) any calculation or appraisal conducted by or on behalf of the **Insurer** pursuant to this Network Interruption Extension.

After: (A) the presentation of the satisfactory written proof of **Network Loss** as provided for in (i), (ii), and (iii) above by the **Insured**; and

(B) the subsequent written acceptance thereof by the **Insurer**,

all adjusted claims are due and payable forty five days (45) thereafter. The costs and expenses of establishing or proving an **Insured's** loss under this Network Interruption Extension, including, without limitation, those

Associated with preparing the proof of loss, shall be the obligation of the **Insured** and not covered under this policy.

### F.5 Net Profit Calculations

In determining the **Network Loss** for the purpose of ascertaining amount payable under this

Network Interruption, due consideration shall be given to the prior experience of the **Company's** business before the beginning of the **Security Failure or System Failure** and to the probable business an **Insured** could have performed had no **Security Failure or System Failure** occurred. **Network Loss** calculations shall not include, and this policy shall not cover, net income that would likely have been earned as a result of an increase in volume of business due to favorable business conditions caused by the impact of security failures on other businesses. Calculations shall be on an hourly basis and based on such an **Insured's** actual net profit loss: caused by a reduction in revenue or increase in charges and expenses directly attributable to the **Material Interruption**.

## **F.6 Appraisal**

If the **Company** and the **Insurer** disagree on the extent of **Network Loss**, either may make a written demand for an appraisal of such Network Loss. If such demand is made, each party will select a competent and impartial appraiser. The appraisers will then jointly select an expert who has not less than ten (10) years' standing and who is a partner in a major international accounting firm, experienced in assessing loss. Each appraiser will separately state the extent of **Network Loss**. If they fail to agree, they will submit their differences to the expert. Any decision by the expert will be final and binding.

The **Company** and the **Insurer** will (i) pay their own respective chosen appraiser and (ii) bear the expenses of the expert equally. Any appraisal of **Network Loss** shall be calculated in accordance with all terms, conditions and exclusions of this policy.

## **G. PCI – DSS**

### **G.1 PCI-DSS Assessment**

In consideration of the additional premium paid the **Insurer** will pay to the company any **PCI DSS Assessment**.

### **G.2 Definitions**

**PCI DSS Assessment** means any written demand received by an **Insured** from a **Card Association** or **Acquiring Bank** for a monetary assessment of a fine or penalty due to an **Insured's** non compliance with **PCI Data Security Standards** resulting from a **Qualifying Breach of a Data Security**.

**Acquiring Bank** means any bank which processes merchant **credit card** transactions and credits those transactions to a merchants account.

**Credit Card** means credit card, debit card, stored value cards and prefunded cards.

**Card Association** means MasterCard, Visa, RuPay, Discover, American Express or JCB.

**PCI Data Security Standards (PCI DSS)** means generally accepted and published Payment Card Industry standards for data security, including but not limited to

(i) Install and maintain a firewall configuration to protect card holder data.



- (ii) Do not use vendor supplied defaults for system passwords and other security parameters.
- (iii) Protect stored card holder data
- (iv) Encrypt transmissions of card holder data across open, public networks.
- (v) Use and regularly update antivirus software
- (vi) Develop and maintain secure systems and applications
- (vii) Restrict access to card holder data by business need to know.
- (viii) Assign a unique ID to each person with computer access.
- (ix) Restrict physical access to card holder data
- (x) Track and monitor all access to networks, resource and card holder data.
- (xi) Regularly test security system and processes
- (xii) Maintain a policy that addresses information security.

## H. REWARD EXPENSES

### H.1 Reward Expenses

It is hereby declared and agreed that the **Insurer** shall pay **Reward Expenses** which is incurred during the **Policy Period**.

### H.2 Definitions

**Reward Expenses** means the reasonable amount paid by an **Insured**, with the prior approval of the **Company**, to an **Informant** for information not otherwise available which leads to the arrest and conviction of persons responsible for a **Cyber Attack, Fraudulent Access or Transmission** or a **Threat** otherwise covered under this policy.

**Informant** means any natural person providing information solely in return for monetary payment paid or promised by an **Insured**

**Cyber Attack** means the transmission of fraudulent or unauthorized **Data** that is designed to modify, alter, damage, destroy, delete, record or transmit information within a **System** without authorization including **Data** that is self replicating or self propagating and is designed to contaminate other computer programs or legitimate computer **Data**, consume computer resources or in some fashion usurp the normal operation of a **System**.

**Fraudulent Access or Transmission** Means that a person has

- (i) Fraudulently accessed an **Insured's System** without authorization
- (ii) **Exceeded Authorized Access**, or
- (iii) launched a **Cyber –attack** into an **Insured's System**

**Threat** means a declaration made by a natural person that he has gained access or alleges to have gained access to an **Insured's system** and intends to;

- (i) Cause an **Insured** to transfer, pay or deliver any funds or property using an **Insured's Systems**
- (ii) Sell or disclose a **Record** to another person
- (iii) Alter, damage or destroy an **Insured's data** while stored within an **Insured's Systems** ;
- (iv) Alter, damage or destroy an **Insured's Data** through a **Cyber Attack**; or
- (v) Impair or deny an **Insured's Services**, and makes a demand for an extortion payment or a series of such payments as conditions for the mitigation or removal of such **Threat**.

**Media** means objects on which **Data** can be stored so that it can be read, retrieved or processed by a **Computer**. **Media** does not mean paper.

**Data** means a representation of information, knowledge, facts, concepts or instructions which are processed or have been processed in a Computer

**Computer** means a device or group of devices that by manipulation of electronic, magnet, optical or electromechanical impulses pursuant to a computer program can perform operations on **Data**.

**System** means a **Computer** and

- (i) all input, output, processing, storage and communication devices controlled, supervised or accessed by the operating systems that are proprietary to, or licensed to, the owner of the **Computer** and

(ii) **Media**

**Exceeded Authorized Access** means to access an **Insured's System** with authorization but to use such access to perform unauthorized fraudulent operations, including the fraudulent input of **Data**.

**Record** means a natural person's first name or first initial and last name, in combination with;

- (i) Their drivers license number, tax file number or other personal identification number (including an employee identification number or student identification number);
- (ii) their financial account number (including a bank account number, superannuation or retirement account number);
- (iii) Medicare card number
- (iv) Their credit, debit or payment card number
- (v) Any information related to their employment by an **Organization**; or
- (vi) Any individually identifiable health information held by an **Organization**.

When any of the information in "A" through "F" above is intended by an **Organization** to be accessible only by persons it has specifically authorized to have such access.

**Organization** means the **Principal Organization** and any subsidiary, or any one of them.

## I. FRAUDULENT COMMUNICATION LOSS

### I.1 Fraudulent Communication Loss

The **Insurer** shall pay Fraudulent Communications Loss which is discovered during the Policy Period.

### I.2 Definitions

**Fraudulent Communication Loss** means loss resulting directly from a Customer, automated clearing house, custodian or financial institution having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value on the faith of any fraudulent Communication purporting to have been directed by an **Insured** to any of the foregoing for the purpose of initiating, authorizing or acknowledging the transfer, payment, delivery or receipt of funds or property, but which Communication was either not sent by an **Insured** or was fraudulently modified during electronic transmission and for which loss an **Insured** is held to be legally liable.

**Communication** means an electronic record or message created, generated, sent, communicated, received or stored by electronic means that is capable of Deductible by the recipient at the time of receipt, including a telefacsimile transmission or e-mail, and that was transmitted or purported to have been transmitted through a Network.

**Network** means any and all services provided by or through the facilities of any electronic or computer communication system, including Fed wire, Clearing House Interbank Payment System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT) and similar automated interbank communication systems, automated teller machines, point of sale terminal and other similar operating systems and includes any share networks, internet access facilities, or other similar facilities for such systems, in which an **Insured** participates, allowing the input, output, examination, or transfer of data or programs from one computer system to an **Insured's** Computer System.

## J. CYBER TERRORISM

**J.1 Cyber Terrorism** means the premeditated use of disruptive activities against any Computer System or network, with the explicit threat to use such activities, that results in causing harm, furthering social, religious, political or similar objectives, or intimidating any person(s) in furtherance of such objectives.

## K. PSYCHOLOGICAL SUPPORT EXPENSES

### K.1 Psychological Support Expenses

The **Insurer** shall pay the Psychological Support Expenses incurred during the Policy Period.

## K.2 Definitions

**Psychological Support Expenses** shall mean any reasonable and necessary fees, costs and expenses incurred by an **Insured**, with the **Insurer's** prior written consent, for psychologist services, in connection with a covered **Claim**.

## L. FRAUDULENT FUND TRANSFER LOSS

### L.1 Fraudulent Fund Transfer Loss

It is hereby declared and agreed that The **Insurer** shall pay **Fraudulent Fund Transfer Loss** which is **discovered** during the **Policy Period**.

### L.2 Definitions

**Fraudulent Fund Transfer Loss** means loss resulting directly from an **Insured** having transferred, paid or delivered any funds or property, established any credit, debited any account or given any value due to the fraudulent input of Data either directly into an **Insured's** System or through a Network into an **Insured's** System.

**Data** Means a representation of information, knowledge, facts, concepts, or instructions which are processed or have been processed in a Computer.

**Computer** means a device or group of devices that by manipulation of electronic, magnetic, optical or electromechanical impulses pursuant to a computer program can perform operations on Data.

**Network** means any and all services provided by or through the facilities of any electronic or computer communication system, including Fed wire, Clearing House Interbank Payment System (CHIPS), Society for Worldwide Interbank Financial Telecommunication (SWIFT) and similar automated interbank communication systems, automated teller machines, point of sale terminals and other similar operating systems and includes any shared networks, internet access facilities, or other similar facilities for such systems, in which an **Insured** participates, allowing the inputs, outputs, examinations, or transfer of Data or programs from one computer to an **Insured's** Computer.

## M. SOCIAL ENGINEERING FRAUD

### M.1 Social Engineering Fraud

The **Insurer** shall indemnify the **Policyholder** for **Loss** resulting from **Social Engineering Fraud** committed during the **Policy Period**.

### M.2 Definitions

**CEO Fraud** Means any fraudulent or dishonest impersonation of a Director, CEO, CFO or their equivalent of the **Policyholder** or a **Subsidiary**, by a **Third Party**, who instructs, via **Electronic**

**Communications**, an **Employee** to execute an authorized fund transfer from the **Policyholder** or a **Subsidiary** account.

**Employee Fraud** Means any fraudulent or dishonest impersonation of an employee of the **Policyholder** or a **Subsidiary**, by a **Third Party** which causes a direct/indirect loss to the **policyholder** or a **subsidiary**.

**Electronic Communications** Means communications that have been transmitted or delivered electronically:

- (i) (a) through an electronic communication system; or
- (b) via the internet, intranet or extranet, provided such communications in (i) (a) or (b) above have been **tested**; or
- (ii) By any other **tested** communication.

**Social Engineering Fraud** Means any **CEO Fraud** and/or any **Vendor Fraud**.

**Tested** means

- (i) A method of authenticating:

The identity of the originator of a communication;

(b) The contents of a communication; or

(c) that the contents of a communication have not been altered or modified during transmission, including the use of digital signatures, public key cryptography, asymmetric cryptography, a Personal Identification Number (PIN), or other similar technologies or encryption methods; or

- (ii) the use of a “call back” to an authorised person, other than the individual initiating the communication, to authenticate the contents of a communication where such communication is a voice communication made over the telephone or by Voice over Internet Protocol (VoIP), or other forms of IP or broadband telephony; or

**Vendor** means a person or entity that provides, or has provided, goods or services to the **Policyholder** or a **Subsidiary** under a written agreement.

**Vendor Fraud** means any fraudulent or dishonest impersonation of a **Vendor** of the **Company**, by a **Third Party**, who instructs, via **Electronic Communications**, an **Employee** to execute an authorized fund transfer from the **Policyholder** or a **Subsidiary** account.

### 3. DEFINITIONS

**3.1 Asset** means any item or element of hardware, software or equipment that is or may be used for the purpose of creating, accessing, processing, protecting, monitoring, storing, retrieving, displaying or transmitting electronic data of any type (including voice).

**3.2 Additional Insured** means Notwithstanding anything contained to the contrary, it is hereby declared and agreed that with effect from the advice received from **Insured** Additional **Insured** stands covered under the policy but only with respect to any liabilities (for which this insurance applies) arising from the business activities covered under this policy and conducted by this additional **Insured** or on their behalf by the named **Insured**.

It is also declared and agreed that each person or party indemnified is separately indemnified in respect of claims made against any of them by any other person or party (other than the named **Insured**) subject to Company's total liability not exceeding the limits of Liability stated in the Schedule of the Policy.

**3.3 Breach Notice Law** means any **Data Protection Law** that creates a legal obligation to give notice in respect of an actual or potential breach.

**3.4 Claim** means the receipt by or service upon the **Insured** of:

- (i) an Enforcement Notice
- (ii) a written demand seeking a legal remedy
- (iii) a demand or notification of civil, regulatory, administrative or criminal proceedings seeking legal remedy, compliance or other sanction or
- (iv) a written demand by a Regulator in connection with a Regulatory Investigation (in respect of Insurance cover B (Administrative Obligations) only).

**Claim** shall not include any (i) Data Subject Access Request or (ii) allegation brought by or on behalf of any director, partner, principal, chief compliance officer, Data Protection Officer or General Counsel of the Company.

**3.5 Company** means the Policyholder and any Subsidiary.

**3.6 Computer Systems** means information technology and communications systems, networks, services and solutions (including all Assets) that either

- (i) form part of such systems and networks, or
- (ii) are used in the provision of such services and solutions which are leased or made available to or accessible by the Company or which are provided to the Company's exclusive and secure usage for the purpose of its business.

"**Computer System** also includes those systems operated by a **third party** for the purpose of providing hosted computer infrastructure or computing platforms to a **Company** as provided in a written contract between such **third party** and a **Company**, including, without limitation, **cloud computing services** provided on an Infrastructure as a Service (IaaS), Software as a Service (SaaS), or Platform as a Service (PaaS) model".

**3.7 Control Group** - Notwithstanding anything herein contained to the contrary, it is hereby agreed and declared that the **Insured** shall deem to have knowledge of claims, events, circumstances, accident, offence or a suit only if the "Control Group" comprising of persons declared by **Insured** have knowledge of the same or the same have been brought to their attention.

**This "Control Group"** shall only comprise of persons who are in active and permanent employment of the client. It is also a condition precedent to this clause that the "Control Group" shall have at least 1 participant member each from the finance department, the administrative department and line control department (not below the rank of a General Manager or equivalent) (for Example- CEO, COO, CFO or equivalent positions of any entity **Insured**)

Even if the claims, events, circumstances, accident, offence or a suit is brought to knowledge of any one member of the control group, it will be deemed to be in knowledge of the entire "control group"

The claims, events, circumstances, accident, offense, or a suit may be deemed to be in knowledge of the "Control Group" if any of its member is notified of the same via E- mail, Facsimile, courier, Registered post and SMS or any other internal mode of communication or external forms of mode of communications via newspaper, TV, radio etc.

**3.8 Corporate Information** means

- (i) any confidential information, which is the exclusive intellectual property of a Third Party including but not limited to budgets, customer lists, marketing plans and other information the release of which would be advantageous to a competitor and which is otherwise not available to such competitors;
- (ii) any information which is confidential or which is subject to legal professional privilege to which a Third Party is entitled including but not limited to any confidential Information supplied to a solicitor, accountant or other professional advisor in the course of his or her professional duties which is otherwise not in the public domain or
- (iii) any information which is lawfully disclosed to the company and which is lawfully received by the company in circumstances which impose a legal obligation to keep the information confidential or which is provided to the Company pursuant to a written confidential agreement, and which has been lawfully collected and maintained by or on behalf of the **company**.

**3.9 Damages** means

- (i) any amount that an **Insured** shall be legally liable to pay to a **Third Party** in respect of judgments or arbitral awards rendered against an **Insured**;
- (ii) monies payable by an **Insured** to a **Third Party** pursuant to a Settlement Agreement negotiated by the **Company** and which is approved by the **Insurer**, pursuant to an act, error or omission on the part of an **Insured**.
- (iii) punitive or exemplary damages where insurable by law
- (iv) Civil fines and penalties where insurable by law

**Damages** shall not mean and this policy shall not cover any

- (i) non-compensatory damages, multiple, liquidated damages
- (ii) the costs and expenses of complying with any order for, grant of or agreement to provide injunctive or other non-monetary relief
- (iii) costs or other amounts that the **Insured** are responsible for under a merchant services agreement
- (iv) discounts, service credits, rebates, price reductions, coupons, prizes, awards or other contractual or non-contractual incentives, promotions or inducements offered to the **Insured's** customers or clients.

**3.10 Data Administrative Fines** means any lawfully insurable fines and penalties which are adjudicated by a **Regulator** to be payable by an **Insured** for a breach of **Data Protection Law**.

**Data Administrative Fines** shall not include any other type of civil or criminal fines and penalties.

**3.11 Data Protection Law** means the applicable laws in **India** and any and all other **equivalent laws** and **regulations** applicable to the **Insured** anywhere in the world and such laws or regulations as may be enacted and/or amended from time to time, relating to the regulation and enforcement of data protection and privacy in any country.

**3.12 Data Protection Officer** means an employee who is designated by the **Company** as the person Officer responsible to implement, monitor, supervise, report upon and disclose the **Company's** regulatory compliance standards with respect to data collection, data processing and delegation of data processing.

**3.13 Data Subjects** means any natural person whose **Personal Information** has been collected or processed by or on behalf of the **Company**.

**3.14 Data Subject Access Request** means a written request from a Data Subject to the Company regarding the mandatory production of:

- (i) **Personal Information** held which identifies such individual person;



- (ii) the reason such **Personal Information** has been collected or processed;
- (iii) the recipients or classes of recipients to whom such **Personal Information** has been or may be disclosed; and
- (iv) the source of such **Personal Information**.

**3.15 Defence Costs** means reasonable and necessary legal fees, costs and expenses which the **Insured** incurs, with the prior written consent of the **Insurer**, in relation to the investigation, response, defence, appeal and/or settlement of a Claim made against the **Insured**.

**Defence Costs** shall not mean any internal costs of the **Insured** (e.g., wages, salaries or other remuneration).

**3.16 Enforcement Notice** means a notice from a Regulator requiring the Company to:

- (i) confirm compliance with the applicable Data Protection Law;
- (ii) take specific measures to comply with the applicable Data Protection Law; or
- (iii) refrain from processing any specified Personal Information or Third Party Data; within a specified time period.

**3.17 Information Commissioner** Such role as may be appointed by the **Regulator** under laws and regulations relating to the regulation and enforcement of data protection and privacy and any equivalent position in any other jurisdiction.

**3.18 Insured** means

- (i) the **Company**
- (ii) any natural person who is or has been a director, principal, partner or officer (including but not limited to any chief compliance officer, **Data Protection Officer** or General Counsel) of the **Company** to the extent such person is acting in such capacity;
- (iii) any employee of the **Company**;
- (iv) subcontractors, to the extent that they are working on behalf of the **Company**;
- (v) entities or third party that the **Company** is required by contract to add as an **Additional Insured** under the policy, but only for the wrongful acts of the Company and any estates or legal representatives of any **Insured** described in (i),(ii),(iii),(iv) and (v) of this definition to the extent that a claim is brought against them in respect of an act, error or omission of such **Insured**.

**3.19 Insurer** means General Insurance Company Limited

**3.20 Limit of Liability** means the amount specified in item 5 of the Schedule.

**3.21 Loss** means

- (i) Damages, Defence Costs, Professional Fees, Data Administrative Fines; and
- (ii) Extortion Loss (if purchased) and
- (iii) Network Loss (if purchased).
- (iv) Inflated telephone bill arising due to unauthorized calls while bank's system being infiltrated by Hacker
- (v) Liability arising from man in the middle attacks and cyber hacking

Loss shall not mean any compensation, internal or overhead expenses of any **Insured** or the cost of any **Insured's** time.

**3.22 Newsworthy Event** means the actual or threatened public communication or reporting in any media which arises directly out of an actual or potential or alleged breach of **Data Protection Law, Qualifying Breach of Personal Information, Qualifying Breach of Corporate Information, Qualifying Breach of Data Security, Material Interruption or Extortion Threat** which is likely to bring the **Company** into disrepute or tarnish its reputation and damage its goodwill amongst the community of people or businesses who are its customers or suppliers or with whom the **Company** habitually deals with in the course of its business.

**3.23 Non Cancellation Clause** means that the policy may not be cancelled except for non-payment of the premium by the Policyholder.

**3.24 Outsourcer** means a natural person or entity which collects or processes **Personal Information or Corporate Information** on behalf of the **Company**, whether based on an express contractual agreement or under a legal requirement.

**3.25 Personal Information** means any private information concerning a **Data Subject** which has been lawfully collected and maintained by or on behalf of the **Company**.

**3.26 Policy Holder** means the entity specified as such in item 1 of the Schedule.

**3.27 Professional Fees** means the reasonable and necessary **fees, costs** and **expense** of **experts** engaged by the **Insured** in accordance with the terms of this policy and with the prior written consent of the **Insurer**.

Provided however, that the **Insured** is permitted to take reasonable and necessary action and incur costs during the first 48 hours of a qualifying breach of data security without the prior consent of the **Insurer**.

**3.28 Qualifying Breach of Corporate Information** means the accidental or negligent disclosure of Corporate Information by an **Insured** for which the company is responsible.

**3.29 Qualifying Breach of Data Security** means the unauthorised access of the **Company's Computer System** or use or access of the **Company's Computer System** outside of the scope of the authority granted by the **Company**.

**3.30 Qualifying Breach of Personal Information** means unauthorised disclosure or transmission by an **Insured** of **Personal Information** for which the Company is responsible as either a Data Processor or a Data Controller as defined under any applicable **Data Protection Law**.

**3.31 Regulator** means not just an **Information Commissioner** or statutory body established pursuant to Data Protection Law in any jurisdiction but also includes relevant sectoral regulators such as **RBI, SEBI** or similar **regulators** and which is authorised to enforce statutory obligations in relation to the processing or control of **Personal Information** (or where relevant, Corporate Information).

**3.32 Regulatory Investigation** means any formal or official action, investigation, inquiry or audit by a Regulator against an **Insured** arising out of the use or alleged misuse of **Personal Information** or any aspects of the control or processing of Personal Information or delegation of data processing to an **Outsourcer** which is regulated by **Data Protection Law**, but shall not include any industry-wide, non-firm specific, inquiry or action.

**3.33 Deductible** means the amounts specified as such in item 7 of the Schedule.

**3.34 Retroactive Date** means the date specified as such in item 9 of the Schedule.

**3.35 Settlement Agreement** means any agreement made by the Company (with the prior written consent of the **Insurer**) with a Third Party, in order to set aside permanently any potential or actual litigious matter or disagreement between the **Insured** and a Third Party.

**3.36 Subsidiary** means any entity in which the Policyholder, either directly or indirectly through one or more of its other entities:

- (i) controls the composition of the board of directors;
- (ii) controls more than half of the voting power; or
- (iii) holds more than half of the issued share or equity capital.

For any Subsidiary or any **Insured** thereof, cover under this policy shall only apply to a breach of Data Protection Law or an act, error, or omission resulting in a Qualifying Breach of Data Security committed while such entity is a Subsidiary of the Policyholder.

**3.37 Third Party** means any natural person or entity who deals at arm's length with the **Insured** and which neither controls or is controlled by the **Insured** and which is not:

- (i) an **Insured**; or
- (ii) any other natural person or entity having a significant financial investment or executive role in the operation or management of the Company;
- (iii) any person or entity who can by virtue of any legal, equitable or commercial right or interest control or influence the board of directors or the management of the Company or which can be influenced or controlled by the Company in a similar manner.

**3.38 Third Party Data** means

- (i) Corporate Information;
- (ii) any private information concerning a natural person, which has been lawfully collected and maintained by or on behalf of a Third Party;
- (iii) any other information of a commercial, business or operational nature belonging to a Third Party, and which is held by the Company under a contractual obligation between the Company and a Third Party in the course of provision of services.

## 4. EXCLUSIONS

The **Insurer** shall not be liable for **Loss** arising out of, based upon or attributable to:

- 4.1 Anti Trust** means any actual or alleged antitrust violation, restraint of trade or unfair competition. This exclusion shall not apply to clause (v) of D1 Multimedia Liability
- 4.2 Bodily Injury and Property Damage** means any:
- (i) physical injury, sickness, disease or death; and if arising out of the foregoing, nervous shock, emotional distress, mental anguish or mental injury, other than mental anguish or mental injury arising from any breach of **Data Protection Law** by the **Company**; or
  - (ii) loss or destruction of tangible property, other than **Third Party Data**, or loss of use thereof, or the physical theft or loss of the **Company's Assets**
- 4.3 Contractual Liability** means any guarantee, warranty, contractual term or liability assumed or accepted by an **Insured** under any contract or agreement (including but not limited to any service credits, rebates, price reductions, coupons, prizes, awards or other contractual or non-contractual incentives, promotions or inducements offered to the **Insured's** customers or clients) except to the extent such liability would have attached to the **Insured** in the absence of such contract or agreement, provided however this exclusion shall not preclude coverage for any PCI - DSS Assessment.
- 4.4 Criminal acts** is deleted in its entirety and is applicable in respect of the Control Group only.
- 4.5 Conduct** means
- (i) any wilful disregard or non-compliance with a ruling, direction or injunction by a court, tribunal, arbitrator or a Regulator within the jurisdiction;
  - (ii) any deliberate, intentional or reckless commission, aiding, abetting or condoning of or conniving in a dishonest, malicious or fraudulent act or a criminal breach of law or regulation; or
  - (iii) any deliberate, intentional or reckless act by any **Insured**; if committed by the **Company's** directors, principals, partners, chief compliance officer, Data Protection Officer or General Counsel whether acting on their own or in collusion with others

The **Insurer** will continue to pay on behalf of an **Insured**, **Defence Costs** under this policy until any of (i) to (iii) above are found by a court, tribunal, arbitrator or regulator to have been committed by an **Insured**. Following such finding the **Insurer** shall be entitled to repayment of any amount paid to the **Insured** under this policy.

**4.6 Intellectual Property** means any infringement of patents and trade secrets or to loss of rights to secure registration of patents due to an unauthorised disclosure.

This Exclusion 4.6 shall not apply to Insurance cover A.2 (Loss of Corporate Information)

**4.7 Intentional Acts** means any intentional or deliberate act by any natural person who is or has been a director, principal, partner or officer (including but not limited to any chief compliance officer, **Data Protection Officer** or General Counsel) of the **Company** that would reasonably be expected to give rise to a **Claim** against an **Insured**;

**4.8 Licensing Fees** means any actual or alleged obligation to make licensing fee or royalty payments, including but not limited to the amount or timeliness of such payments unless covered under definition of Damages

**4.9 Prior Claims and Circumstances** means any circumstances that, as of the inception date of this policy, may reasonably have been expected by any **Insured** to give rise to a **Claim**, or any **Claim** made or circumstance notified prior to or pending at the inception date of this policy.

**4.10 Terrorism** means any form of war terrorism or riot, provided however that this exclusion shall not apply to actual, alleged or threatened Cyber Terrorism or Cyber Extortion

**4.11 Trading Losses** means any trading losses or trading liability, monetary value of any electronic fund transfers or transactions by or on behalf of the **Insured** which is lost diminished or damaged during transfer from, into or between accounts, or the face value of coupons, price discounts, prizes, awards, or any other valuable considerations given in excess of the total contracted or expected amount is excluded, however, trading losses of **third party** are covered.

**4.12 Unauthorised Trading** means any actual or alleged trading by the **Insured** which at the time of the trade:

- (i) is in excess of permitted financial limits or ;
- (ii) is outside permitted product lines

**4.13 Unsolicited Materials** means any distribution of unsolicited email, direct mail, or facsimiles, wire tapping, audio or video recording, or telemarketing;

**4.14 Uninsurable Loss** means any matters which may be deemed uninsurable under the law governing this policy or the jurisdiction in which a **Claim** is brought or where any Insuring clause or Extension is triggered.

## 5. CLAIMS

### 5.1 Extended Reporting Period

If the **Insurer** cancels or does not renew this policy, other than for non-payment of Premium or any other breach of the terms of this policy by an **Insured**, the Policyholder shall have the right to a period of 90 days following the date of cancellation or expiry in which to give notice of any covered Claim first made against the **Insured**. That extended reporting period shall not apply if this policy or its cover has been replaced.

The reporting period can be further extended to 365 days by paying additional premium of 100% of the annual premium. Any additional period beyond 365 days shall earn a premium not higher than pro-rata but at the sole discretion of the insurer

### 5.2 Fraudulent Claims

If any **Insured** shall give any notice or claim cover for any **Loss** under this policy knowing such notice or claim to be false or fraudulent as regards amounts or otherwise, such **Loss** shall be excluded from cover under the policy, and the **Insurer** shall have the right, in its sole and absolute discretion, to avoid its obligations under or void this policy in its entirety, and in such case, all cover for **Loss** under the policy shall be forfeited and all premium deemed fully earned and non-refundable.

### 5.3 Notification of Claims and Circumstances that may lead to a Claim

This policy affords cover solely with respect to:

- (i) Claims which are first made against the **Insured** during the Policy Period; and
- (ii) Qualifying Breaches of Data Security, breaches of Data Protection

Law, Newsworthy Events, Extortion Threats or Material Interruptions which occur during the Policy Period, and in all events which are reported by the **Insured** in writing to the **Insurer** as soon as practicable and in any case during the Policy Period.

If, during the **Policy Period**, any **Insured** becomes aware of any fact, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law**, **Newsworthy Event**, **Extortion Threat** or **Material Interruption** that an informed person operating within the same type of business as the **Company** would reasonably believe is likely to give rise at a later date to a **Claim**, the **Insured** shall promptly inform the **Insurer** about those circumstances. Such notification must be presented in chronological order and must detail the facts or matters which have or may give rise to a **Claim** which should include at a minimum the following information:

- a. the nature and circumstances of the facts;
- b. alleged, supposed or potential breach;
- c. date, time and place of the alleged, supposed or potential breach;
- d. the identity of the potential claimants and all other potentially involved persons and/or entities;
- e. estimate of possible loss;
- f. the potential media or regulatory consequences.

All notifications relating to **Claims**, circumstances, **Qualifying Breaches of Data Security**, breaches of **Data Protection Law, Newsworthy Events, Extortion Threats** or **Material Interruptions** must be in writing and sent by e-mail, fax or post to:

#### 5.4 Related Claims

If notice of a **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** is given to the **Insurer** pursuant to the terms and conditions of this policy, then:

- (i) Any subsequent **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** alleging, arising out of, based upon or attributable to the facts alleged in that previously notified **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** ; and
- (ii) Any subsequent **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** alleging any **Loss** which is the same as or related to any **Loss** alleged in that previously notified **Claim**, circumstance, **Qualifying Breach of Data Security, Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption**,

Shall be considered made against the **Insured** and reported to the **Insurer** at the time notice was first given.

Any **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** arising out of, based upon or attributable to: shall be considered made against the **Insured** and reported to the **Insurer** at the time notice was first given. Any **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** arising out of, based upon or attributable to:

- (i). The same cause; or
- (ii). A single **Loss**; or
- (iii). A series of continuous, repeated or related **Losses**;

Shall be considered a single **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law, Newsworthy Event, Extortion Threat** or **Material Interruption** for the purposes of this policy.



## 6. DEFENCE AND SETTLEMENT

### 6.1 Defence

The **Insurer** does not assume any duty to defend, and the **Insured** must defend and contest any **Claim** made against it unless the **Insurer**, in its sole and absolute discretion, elects in writing to take over and conduct the defence and settlement of any **Claim**. If the **Insurer** does not so elect, it shall be entitled, but not required, to participate fully in such defence and the negotiation of any settlement that involves or appears reasonably likely to involve the **Insurer**.

The **Insured** must render all reasonable assistance to the **Insurer** and take all reasonable measures to mitigate or avoid the **Loss** or to determine the **Insurer's** liability under the policy.

### 6.2 Insurer's Consent

As a condition precedent to cover under this policy, no **Insured** shall admit or assume any liability, enter into any settlement agreement, consent to any judgment, or incur any **Defence Costs** or **Professional Fees** without the prior written consent of the **Insurer**. Only those settlements, judgments and **Defence Costs** or **Professional Fees** consented to by the **Insurer**, and judgments resulting from **Claims** defended in accordance with this policy, shall be recoverable as **Loss** under this policy. The **Insurer's** consent shall not be unreasonably withheld, provided that the **Insurer** shall be entitled to exercise all of its rights under the policy. Compliance with a **Breach Notice Law** will not be considered as an admission of liability for the purposes of this clause.

### 6.3 Insured's Consent

The **Insurer** may make any settlement of any **Claim** it deems expedient with respect to any **Insured**, subject to such **Insured's** written consent (which shall not be unreasonably withheld or denied). If any **Insured** withholds consent to such settlement, the **Insurer's** liability for all **Loss** on account of such **Claim** shall not exceed the amount for which the **Insurer** could have settled such **Claim**, plus **Defence Costs** incurred as of the date such settlement was proposed in writing by the **Insurer**, less coinsurance (if any) and the applicable **Deductible**.

### 6.4 Subrogation and Recovery

If the **Insurer** makes any payment under this policy, it shall be subrogated to the extent of such payment to all of the **Insured's** rights of recovery and shall be entitled to pursue and enforce such rights in the **Insured's** name, even if the **Insured** is compensated for such **Loss**.

Subrogation against employees (including directors, officers, partners or principals) of the Company shall be limited to cases where such employees have been found guilty of an intentional, fraudulent or criminal act by any court or government entity.

The **Insured** shall provide the **Insurer** with all reasonable assistance and shall do everything that may be necessary to secure any rights including the execution of documents necessary for the **Insurer** to bring suit in the **Insured**'s name. Any amount recovered in excess of the **Insurer**'s total payment shall be restored to the **Insured** less the recovery cost.

“Notwithstanding the foregoing, where the **Insured** agrees in a contract or agreement to waive the **Insurer**'s rights of subrogation against another party, and that contract or agreement is entered into prior to any wrongful act by such other party, the **Insurer**'s rights of subrogation against such other party shall be waived.”

## 7. LIMIT OF LIABILITY AND DEDUCTIBLE

### 7.1 Limit of Liability

The total amount payable by the **Insurer** under this policy shall not exceed the **Limit of Liability**. Sub-limits of Liability, Extensions, **Professional Fees** and **Defence Costs** are part of that amount and are not payable in addition to the **Limit of Liability**. The inclusion of more than one **Insured** under this policy does not operate to increase the total amount payable by the **Insurer** under this policy.

### 7.2 Deductible

With respect to all **claims** or **qualifying breaches of data security**, breaches of **Data Protection Law, Material interruptions** or **Extortions Threats**, the **Insured** will only pay that amount of any loss which is in excess of the deductible specified in the schedule. The deductible amount is to be borne by the company and shall remain uninsured. A single **deductible** shall apply to **Loss** arising from **Claims, Qualifying Breach of Data Security**, breaches of **Data Protections Law, Material Interruptions** or **Extortion Threats** which are considered related **Claims, Qualifying Breaches of data security**, breaches of **Data Protection Law, Material Interruptions** or **Extortion Threats** pursuant to clause 5.4 “**Related Claims**”

In the event that a **Claim, Qualifying Breach of Data Security**, breaches of **Data Protection Law, Material Interruptions** or **Extortions Threats**, triggers more than one of the **deductible** amount, then, as to that **Claims, Breach of data protection law, qualifying breach of data security, Material interruptions** or **Extortions Threats**; Deductible amount mentioned in schedule shall be deemed the Deductible applicable to loss Arising from such claim, breaches of data protection law, qualifying breach of data security, Material interruptions or Extortions Threats.

## 8. GENERAL PROVISIONS

### 8.1 Automatic Acquisition Clause

Subject to all other terms, conditions and exclusions, this Policy is automatically extended to indemnify any firm acquired or created by the **Insured** during the Policy Period provided that:

- (i) In the 12 month period immediately preceding an acquired firm's acquisition, its fee income did not exceed 25 % of the **Insured's** declared fee income for the most recent financial year.
- (ii) The activities of an acquired firm are of a similar type as those undertaken by the Policy holder.
- (iii) In the five year period immediately preceding the acquisition, it has had no claim or loss.
- (iv) The **Insured** has undertaken due diligence prior to any such acquisition and that the due diligence exercise has not identified any potential liabilities which could result in a claim under this Policy.
- (v) An acquired firm is both incorporated in the EU and carries out all its business activities outside of the USA or Canada.

Any firm acquired or created by the **Insured** which does not satisfy the above conditions shall be referred to the **Insurer** to assess and evaluate. The **Insurer** may, but has no obligation to, extend cover provided by the policy to the firm acquired or created. Such extension may be subject to such terms and conditions and additional premium as the **Insurer**, in its absolute discretion, shall deem appropriate.

### 8.2 Cooperation

The **Insured** will at its own cost:

- (i) Render all reasonable assistance to the **Insurer** and co-operate in the defence of any Claim and the assertion of indemnification and contribution rights;
- (ii) Use due diligence and do and concur in doing all things reasonably practicable to avoid or diminish any Loss under this policy;

Give such information and assistance to the **Insurer** as the **Insurer** may reasonably require to enable it to investigate any Loss or determine the **Insurer's** liability under this policy.

### 8.3 Maintenance of Security

The **Insured** will take all reasonable steps to maintain data and information security procedures to no lesser standard than disclosed in the proposal form.

The **Insured** will ensure that back-up systems and processes are maintained to no lesser standard than disclosed in the proposal form and that the ability to restore such data is regularly tested (at least every six (6) months).

#### **8.4 Economic Sanctions**

The **Insurer** is not liable to make any payments for liability under any coverage sections of this policy or make any payments under any extension for any **Loss** or **Claim** arising in, or where the **Insured** or any beneficiary under the policy is a citizen or instrumentality of the government of, any country(ies) against which any laws and/or regulations governing this policy and/or the **Insurer** or the **ReInsurer**, its parent company or its ultimate controlling entity have established an embargo or other form of economic sanction which have the effect of prohibiting the **Insurer** to provide insurance coverage, transacting business with or otherwise offering economic benefits to the **Insured** or any other beneficiary under the policy.

It is further understood and agreed that no benefits or payments will be made to any beneficiary(ies) who is/are declared unable to receive economic benefits under the laws and/or regulations governing this policy and/or the **Insurer** or the **ReInsurer**, its parent company or its ultimate controlling entity.

#### **8.5 Policy Purchase**

In granting cover to the **Insured**, the **Insurer** has relied upon the material statements and particulars in the proposal together with its attachments and other information supplied. These statements, attachments and information are the basis of cover and shall be considered incorporated and constituting part of this policy. In the event of the **Insurer** being entitled to avoid this policy from the inception date or from the time of any variation in cover, the **Insurer** may at its discretion maintain this policy in full force, but exclude the consequences of any **Claim**, circumstance, **Qualifying Breach of Data Security**, breach of **Data Protection Law**, **Newsworthy Event**, **Extortion Threat** or **Material Interruption** relating to any matter which ought to have been disclosed before the inception date or before any variation in cover.

#### **8.6 Assignment**

This policy and any rights under or in respect of it cannot be assigned without the prior written consent of the **Insurer**.

#### **8.7 Cancellation**

##### **By Policyholder:**

This policy may be cancelled by the **Policyholder**. If no **Claim**, **Qualifying Breach of Data Security**, breach of **Data Protection Law**, **Material Interruption** or **Extortion Threat** has been made and no circumstance has been notified prior to such cancellation, the **Insurer** shall

retain x% of the original premium plus the pro-rata proportion due for time on risk. Otherwise, the premium shall not be returned and shall be deemed fully earned at the inception date.

#### **8.8 Insolvency**

Insolvency, receivership or bankruptcy of any **Insured** shall not relieve the **Insurer** of any of its obligations hereunder.

#### **8.9 Plurals, Headings and Titles**

The descriptions in the headings and titles of this policy are solely for reference and convenience and do not lend any meaning to this contract. Words and expressions in the singular shall include the plural and vice versa. In this policy, words in **bold** typeface have special meaning and are defined or specifically mentioned in the Schedule. Words that are not specifically defined in this policy have the meaning normally attributed to them.

#### **8.10 Governing Law**

Any interpretation of this policy relating to its construction, validity or operation shall be made in accordance with the laws of India and in accordance with the English text as it appears in this policy.

#### **8.11 Arbitration**

Any and all disputes or differences which may arise under, out of, in connection with or in relation to this policy, or to its existence, validity or termination, or to the determination of the amount or any amounts payable under this policy, shall be referred to a sole arbitrator to be appointed by the parties to the dispute within 30 days of any party giving notice of arbitration to the other(s).

In the event that the parties are unable to agree upon the identity of a sole arbitrator, the disputes or differences shall be referred to the decision of 3 arbitrators of whom one shall be appointed in writing by each of the parties within a period of 30 days after the failure to appoint a sole arbitrator and the third (who shall serve as Chairman) shall be appointed by the nominated arbitrators. In case either party shall refuse or fail to appoint an arbitrator within the aforesaid 30 days after receipt of notice in writing requiring an appointment, the other party shall be at liberty to appoint a sole arbitrator who shall thereafter be empowered to conduct the arbitration and determine the disputes or differences referred to him as if he had been appointed a sole arbitrator with the consent of both parties.

The parties shall share the expenses of the arbitrator or arbitral tribunal equally and such expenses, along with the reasonable costs of the parties in the arbitration, shall be awarded by the arbitrator or arbitral tribunal in favour of the successful party in the arbitration or, where no party can be said to have been wholly successful, to the party who has substantially succeeded. The place of arbitration shall be India, the language of the arbitration shall be

English, the law applicable to and in the arbitration shall be Indian law and the arbitration process will be in accordance with the provisions of the Arbitration & Conciliation Act 1996, as amended from time to time. It is a condition precedent to any right of action or suit upon this policy that the award by such arbitrator or arbitrators shall be first obtained. In the event that these arbitration provisions shall be held to be invalid then all such disputes shall be referred to the exclusive jurisdiction of the Indian courts.

#### **8.12 Non Rescindable Clause**

The Company shall not be entitled, under any circumstances, to avoid or rescind Insuring Clause A - M with respect to any **Insured** or exercise any rights against any **Insured** for any misrepresentation in the **Proposal** or for any non-disclosure (whether such misrepresentation is innocent, negligent, fraudulent or otherwise). However in the event of misrepresentation or nondisclosure which would otherwise entitle the Company to avoid or rescind this policy or exercise any rights as against one or more **Insured's**:

- (i) No **Insured Person** who, at the time the contract evidenced by this policy was entered into, knew the true position with regard to the facts or matters misrepresented to the Company or knew any of the non-disclosed facts, and no **Organization** to the extent that it may indemnify any such **Insured Person**, shall have cover under this policy for any **Loss** of that **Insured Person** on account of a **Claim** based upon, arising from or in consequence of the true position or any non-disclosed facts; and
- (ii) if any chairman, chief executive officer, chief financial officer, in-house general counsel or the holder of any equivalent position in any jurisdiction of an **Organization** knew the true position with regard to the facts or matters misrepresented to the Company or knew any of the non-disclosed facts, then no **Organization** shall have cover under this policy for any **Loss** of that **Organization** on account of a **Claim** based upon, arising from or in consequence of the true position or any non-disclosed facts.

**8.13** The policy will cover claims in relation to undiscovered past issues not known to insured that may impact during the policy period.

**8.14** It is hereby declared and agreed that the territory and jurisdiction applicable for this policy will be worldwide including USA and Canada.

**NON DISCLOSURE: It is hereby agreed that all the parties in this agreement hereby agree as follows.**

Bidder shall hold all information about this tender and / or information gathered about the Bank through this process in strict confidence with the same degree of care with which Bidder protects it's own confidential and proprietary information. Bidder shall restrict disclosure of the information

solely to its employees, agents and Sub contractors on a need to know basis and advise those persons of their obligations hereunder with respect to such information.

i. To use the information only as needed for the purpose solely related to the project.

ii. Except for the purpose of execution of this project, not disclosure or otherwise provide such information.

iii. Bidder shall not disclose any information to parties not involved in supply of the products and services forming part of this order will be treated as breach of contract and disqualification of the contractor and disqualification of the contractor in any future tendering process of the Bank.

iv. Any information considered sensitive must be protected by the Bidder from unauthorized disclosure or access.

## **SEVERABILITY**

i. If any of the provisions of this Agreement may be constructed in more than one way, one of which would render the provision illegal or otherwise voidable or unenforceable, such provision shall have the meaning that renders it valid and enforceable.

ii. In the event any court or other government authority shall determine any provisions in this agreement is not amended so that it is enforceable to the fullest extent permissible under the laws and public policies of the jurisdiction in which enforcement is sought and affords the parties the same basic rights and obligations and has the same economic effect as prior to amendment.

iii. In the event that any of the provisions of this Agreement shall be found to be void, but would be valid if some part thereof was deleted or the scope period or area of application were reduced, then such provision shall apply with the deletion of such words or such reduction of scope, period, or area of application as may be required to make such provisions valid and effective, provided however that on the revocation, removal or diminution of the law or provisions, as the case may be, by virtue of which such provisions contained in this RFP were limited as provided here in above, the original provisions would stand renewed and be effective to their original extent, as if they had not been limited by the law or provisions revoked. Notwithstanding the limitation of this provision by any law for the time being in force, the parties undertake to at all times observe and be bound by the spirit of this RFP.



## Part II: Quote Slip and Draft Policy wordings

### QUOTE SLIP

Policy Type	Cyber Risk Insurance Policy
Named Insured	Bank of Maharashtra
Territory & Jurisdiction	Worldwide
Communication Address	Bank of Maharashtra 1501, Lokmangal, Shivajinagar, Pune- 411005
Period of Insurance	26 <sup>th</sup> November 2019 to 25 <sup>th</sup> November 2020
Retroactive Date	26 <sup>th</sup> September 2017
Business Description	Banking and Financial Services
Currency of Quote	Rs. 75 Crores
Indemnity Limit	Rs. 75 Crores
Deductible	Option 1 : Rs 25 Lakhs Option 2 : Rs 15 Lakhs
Coverages	
1.	Data Liability
2.	Administrative Obligations
3.	Reputation & Response Cost
4.	Multimedia Liability
5.	Cyber / Privacy Extortion
6.	Network Interruption
7.	PCI DSS Assessment
8.	Reward Expenses
9.	Fraudulent Communication Loss
10.	Cyber Terrorism
11.	Psychological Support Expenses
12.	Fraudulent Fund Transfer Loss
13.	Social Engineering Fraud

Authorized Signatory

**Name:**

**Designation:**

**Vendor's Corporate Name**

**Address**

**Email and Phone #**

## Annexure B: Commercial Bid Format

(To be submitted in Commercial Bid)

To

The CISO  
Bank of Maharashtra  
1501, Lokmangal, Shivajinagar,  
Pune- 411005

Dear Sir,

### **Sub: Response to RFP in connection with Procurement of Cyber Risk Insurance Policy of the Bank**

With reference to the RFP dated 4<sup>th</sup> November 2019 for Cyber Risk Insurance Policy of M/s Bank of Maharashtra we hereby agree to the all the terms and condition as stated in the RFP document, Quote Slip, Policy wordings and all the other annexures. The commercial offer submitted to the Bank is after getting the required approvals from the Competent Authorities of our company.

Description	Sum Insured (Rs.)	Deductible Amount (Rs.)	Net Premium (Rs.)	GST (Rs.)	Total Premium Payable (Rs.)
Cyber Risk Insurance	75 Crores	Option 1 : 25 Lakhs Option 2 : 15 Lakhs			

We confirm that the offer is in conformity with the terms and conditions as mentioned in this RFP. We further confirm that the information furnished in the proposal, annexure, formats, is correct. Bank may make its own inquiries for verification and we understand that the Bank has the right to disqualify and reject the proposal, if any of the information furnished in the proposal is not correct. We also confirm that the prices offered shall remain fixed for a period of 60 days from the date of submission of the offer.

We also understand that the Bank is not bound to accept the offer either in part or in full. If the Bank rejects the offer in full or in part the Bank may do so without assigning any reasons there for.

Yours faithfully,

**Authorized Signatories**  
**(Name, Designation and Seal of the Company)**

**Date:**

### 30 Annexure C – Bid Query Format

Bidders have to provide their queries on eligibility criteria, scope of work, terms & conditions etc. in excel format as mentioned below. Bidders are requested to categorize their queries under appropriate headings. Bidders are requested to provide a reference of the page number, state the clarification point and the queries/suggestions that they propose as shown below (all the pre bid queries will be entertained in this Microsoft Excel format by e-mail):

Bidder Name	Clause Number	Page Number	Clause	Query	Bank Response
-------------	---------------	-------------	--------	-------	---------------

**Date:**

**Signature:**

**Name & Designation:**

**Business Address:**

**31 Annexure D: Covering Letter (to the Bank on the bidder's letterhead)**

To

The Asstt.General Manager,  
Bank of Maharashtra,  
Corporate Services,  
1501, Lokmangal, Shivajinagar,  
Pune- 411005

Dear Sir,

**Sub: Response to RFP in connection with Cyber Risk Insurance Policy of the bank**

With reference to the above RFP, having examined and understood the instructions, terms and conditions, we hereby enclose our offer for Cyber Risk Insurance Policy of the Bank, as detailed in your above referred inquiry. We confirm that the offer is in conformity with the terms and conditions as mentioned in your above referred RFP. We further confirm that the information furnished in the proposal, annexure, formats, is correct. Bank may make its own inquiries for verification and we understand that the Bank has the right to disqualify and reject the proposal, if any of the information furnished in the proposal is not correct.

We also confirm that the prices offered shall remain fixed for a period of 60 days from the date of submission of the offer. We also understand that the Bank is not bound to accept the offer either in part or in full. If the Bank rejects the offer in full or in part, the Bank may do so without assigning any reasons thereof.

Yours faithfully,

**Authorized Signatories**

**(Name, Designation and Seal of the Company)**

**Date:**

## **32 Annexure E - Undertaking by Bidder**

To,

The Asstt.General Manager,  
Bank of Maharashtra,  
Corporate Services .  
1501, Lokmangal, Shivajinagar,  
Pune- 411005

### **Undertaking (To be submitted by all Bidders' on their letter head)**

We \_\_\_\_\_(bidder name), hereby undertake that-

- 1 As on date of submission of tender, we are not blacklisted by the IRDAI/RBI/IBA Central Government / any of the State Governments in India.
- 2 We also undertake that, we are not involved in any legal case that may affect the solvency / existence of our firm or in any other way that may affect capability to provide / continue the services to bank.

Yours faithfully,

**Authorized Signatories**

**(Name, Designation and Seal of the Company)**

**Date:**