

# Standard Bidding Document

## OGDCL Cyber Risk Reinsurance Coverage (Non-Consultancy Services)

International

Single Stage-Two Envelope



*June 07, 2026*

*Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist  
PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi  
(Division), Sindh (Province).  
Phone: +92-300-699-8576, Email: aghafoor@pakre.org.pk*

# Table of Contents

---

|   |    |
|---|----|
| <b>Instructions to Bidders</b> .....        | 3  |
| <b>Bid Data Sheet</b> .....                 | 24 |
| Bids Data Sheet (BDS) .....                 | 25 |
| Eligibility Criteria .....                  | 29 |
| Evaluation Criteria .....                   | 29 |
| Required Services .....                     | 31 |
| Related Services : .....                    | 31 |
| Services Specifications .....               | 31 |
| Scope of Work .....                         | 32 |
| Price Schedule .....                        | 32 |
| <b>General Conditions of Contract</b> ..... | 34 |
| <b>Special Conditions of Contract</b> ..... | 44 |
| <b>Bid Securing Declaration</b> .....       | 49 |
| <b>Contract Form</b> .....                  | 51 |
| <b>Integrity Pact</b> .....                 | 54 |
| <b>Performance Guarantee Form</b> .....     | 56 |
| <b>Annexure</b> .....                       | 58 |
| Terms & Conditions .....                    | 59 |
| Policy Wording .....                        | 59 |
| Proposal Form .....                         | 59 |
| Technical Evaluation Criteria .....         | 59 |

|   |    |
|---|----|
| Financial Matrix .....                      | 59 |
| <b>Procurement Forms</b> .....              | 61 |
| <b>Additional Forms and Documents</b> ..... | 64 |

## PROCUREMENT NOTICE

# PROCUREMENT OF NON-CONSULTANCY SERVICES

1. The **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce)** has reserved Funds for the procurement planned for FY **2026-27**. The **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce)** intends to apply part of the proceeds of this Fund to cover eligible payments under the contract for the “**OGDCL Cyber Risk Reinsurance Coverage**”

2. The **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce)** invites Bids through **EPADS v2.0** from eligible Bidders registered on **EPADS v2.0** for provision of Non-Consultancy Services.

3. **Single Stage-Two Envelope** Procedure of Principal Method of Procurement (i.e. Open Competitive Bidding) will be used by adopting **Least Cost Based Selection (LCBS)** Technique for the subject procurement, in line with the Public Procurement Rules, 2004 and any Regulations, and Instructions issued by the Authority (from time to time).

4. All Bids must be accompanied by a Bid Security described in Bid Security Section in Bidding Document in the form of **Pay Order, Bank Guarantee, Others** or Bid Securing Declaration on the prescribed format described.

5. E-Bidding documents, containing detailed terms & conditions, specifications and requirements etc. are available on **e-Pak Acquisition and Disposal System (EPADS)** at <https://vendors.epads.gov.pk/>.

6. The e-bids, prepared in accordance with the instructions in the e-Bidding documents, must be submitted through **EPADS v2.0** on or before **Tuesday, July 7, 2026 11:00 AM**. E-bids will be opened on the same day at **Tuesday, July 7, 2026 11:30 AM**. Manual submission of Bids shall not be entertained. Those vendors who have not yet registered on the new version of **EPADS v2.0**, may register themselves on <https://vendors.epads.gov.pk/>. A tutorial to explain the registration process is available at <https://www.youtube.com/watch?v=MNW6T38v7tc>

7. In terms of Rules 48 of Public Procurement Rules, 2004 Grievance Redressal Committee (GRC) is notified for the subject procurement and notification copy is

available on the procuring agency's website and also available on **EPADS v2.0** as well as Authority's website at ([www.ppra.org.pk](http://www.ppra.org.pk)).

Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce),  
Procurement Specialist

PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi  
South (District), Karachi (Division), Sindh (Province).

+92-300-699-8576

aghafoor@pakre.org.pk





## Instructions to Bidders

## A. Introduction

### 1. Scope of Bids

1.1. The Procuring Agency (PA), as indicated in the **Bids Data Sheet (BDS)** invites Bids through **EPADS v2.0** for the provision of Non-Consultancy Services for as specified in the BDS and **in Section Evaluation Criteria, Specifications & Schedule of Requirements**. The name, identification, and number of items/deliverables are provided in the **BDS**. **Single Stage-Two Envelope** procedure of the open competitive method shall be used. The successful Bidders will be expected to provide the services within the specified period and timeline(s) as stated in the **BDS**.

### 2. Source of Funds

2.1. Source of funds is referred in Clause-1 of Invitation for Bids.

### 3. Fraudulent & Corrupt Practices

3.1. As defined under Rule 2(1)(f) of the Public Procurement Rules, 2004.

### 4. Eligible Bidders

4.1. A bidder is eligible to participate in a procurement process if the bidder:

4.1.1. possesses or has access to the technical competence, financial resources, equipment and other physical facilities, personnel, managerial capability, experience and reputation necessary to complete the procurement contract;

4.1.2. has the legal capacity to enter into a procurement contract;

4.1.3. is not insolvent, in receivership, bankrupt or being wound up and its activities or affairs are not suspended or being administered under any Act, by a court or by a judicial officer;

4.1.4. is not the subject of legal proceedings for any of the matters mentioned in sub-rule (c);

4.1.5. has fulfilled or has made substantial arrangements satisfactory to the relevant authorities, to fulfil its obligations to pay taxes and social security (where applicable) other contributions of its employees; and

4.1.6. has not, or in the case of a company, its owners and beneficial owners, directors or officers have not, been convicted of a criminal offence related to:

4.1.6.1. its professional conduct; or

4.1.6.2. a bidder (or, in the case of a company, its key individuals such as owners, beneficial owners, directors, or officers) must not have engaged in any prohibited practice, such as fraud, corruption, collusion, or coercion, within the time period stated in the bidding documents, which can be up to three years before the start of the procurement process. Additionally, the bidder must not have been debarred (i.e., banned) from participating in public procurement processes in Pakistan or by any international organization or country. If they have, they are ineligible to participate in the current bidding.

4.2. The procuring agency may require a bidder participating in the procurement process to provide the prescribed documentary evidence or other information to satisfy itself that the bidder is qualified in accordance with the criteria in sub-clause (1).

4.3. A procuring agency shall set out in the bidding document all the criteria for qualification to be applied in accordance with sub-clause (1).

4.4. Except as permitted under the Ordinance, Rules and Regulations, the procuring agency shall not establish a criterion for eligibility of a bidder that:

4.4.1. discriminates against or among a bidder or against categories of bidders; or

4.4.2. is not required for the performance of the procurement contract; or

4.4.3. is not related to the avoidance or management of legal, reputational or economic risk to the procuring agency unless it is in the national interest to do so, and the criteria is set out in the bidding documents.

4.5. A procuring agency shall assess the eligibility of a bidder for participation in the procurement process against the criteria for qualification under sub-clause (1).

4.6. In the case of a joint venture, consortium, or association, all members shall be jointly and severally liable for the execution of the contract in accordance with the terms and conditions of the contract. The joint venture, consortium, or association shall nominate a lead member as nominated in the BDS,

4.7. who shall have the Authority to conduct all business for and on behalf of any and all the members of Joint venture, consortium, or association during the bidding process, and in case of award of contract, during the execution of the contract.

4.8. The appointment of the lead Member in the joint venture, consortium, or association shall be confirmed by submission of valid power of Attorney to the procuring agency.

4.9. Subject to the limits specified in the BDS, the procuring agency may allow bidders to participate in the form of a Joint Venture (JV). However, each party in the JV must individually meet the eligibility criteria specified in the BDS

4.10. No Bidder can be a sub-contractor while submitting a Bids individually or as a member of a joint venture in the same Bidding process.

## **5. Qualification of the Bidder**

5.1. All Bidders shall provide in Section VI, Bid Forms, a preliminary description of the proposed work method and schedule, including drawings and charts, as necessary.

## **B. Bidding Documents**

## 1. Contents of Standard Bidding Document

1.1. The Services required, bidding procedure, and terms and conditions of the contract are prescribed in the bidding document. In addition to the Invitation for Bids, the bidding document which should be read in conjunction with any addendum issued by the Procuring Agency include:

**Section I** - Invitation to Bid

**Section II** Instructions to Bidders (ITB)

**Section III** Bid Data Sheet (BDS)

**Section IV** Eligible Countries

**Section V** Evaluation Criteria, Specifications, Schedule of Requirements, and Technical Specifications.

**Section VI** Bidding Forms

**Section VII** Fraudulent & Corrupt Practices

**Section VIII - Material & Non-material deviation**

**Section IX** General Conditions of Contract (GCC)

**Section X** Special Conditions of Contract (SCC)

**Section XI** Contract Forms

1.2. The Bidder is expected to examine all instructions, requirements, forms, terms and specifications in the bidding documents. Failure to furnish all the information required in the bidding document will be at the Service provider's risk and may result in the rejection of his bids.

## 2. Clarifications

2.1. Clarifications of the bidding documents may be requested in writing through EPADS v2.0 by any bidder up to three days prior to the deadline for the submission of bids.

The procuring agency shall respond promptly and in writing to any request by a bidder for clarification of the bidding documents and, in any event, no later than two days prior to the deadline for the submission of bids or proposals.

Responses to requests for clarification shall be communicated simultaneously and in writing to all bidders participating in the procurement proceedings.

No bidder shall be allowed to alter or modify his bid after the bids have been opened however, the procuring agency may seek and accept clarification to the bid that do not change the substance of the bid, through EPADS v2.0.

2.2. Procuring Agency's response will be uploaded on the EPADS v2.0, including a description of the inquiry.

2.3. Should the Procuring Agency deem it necessary to amend the bidding document as a result of a clarification, it shall do so following the procedure under **ITB 1.1.**

2.4. If indicated **in the BDS**, the bidder's designated representative is invited at the bidder's cost to attend a pre-bid meeting at the place, date and time mentioned **in the BDS**. During this pre-bid meeting, prospective bidder(s) may request clarification(s) regarding the schedule of requirements, the Evaluation Criteria or any other aspects of the bidding document.

2.5. Minutes of the pre-bid meeting, if applicable, including the text of the questions asked by bidders, and the responses given, together with any responses prepared after the meeting will be uploaded on EPADS v2.0. Any modification to the bidding document that may become necessary as a result of the pre-bid meeting shall be made by the Procuring Agency exclusively through the use of an Addendum.

2.6. To assist in the examination, evaluation and comparison of Bids of the Bidders, the Procuring Agency may, ask any Bidder for a clarification of its bid including breakdown of prices, through EPADS v2.0. Any clarification submitted by a bidder that is not in response to a request by the Procuring Agency shall not be considered.

No change in the prices or substance of the bid shall be sought, offered, or permitted.

The alteration or modification in the bid which in any way affect the following parameters will be considered as a change in the substance of a

bid:

- 2.6.1. evaluation & qualification criteria;
- 2.6.2. required scope of work or specifications;
- 2.6.3. all securities requirements;
- 2.6.4. tax requirements;
- 2.6.5. terms and conditions of bidding documents; and
- 2.6.6. change in the ranking of the bidders.

From the time of bid(s) opening to the time of contract award, if any bidder wishes to contact the procuring agency on any matter related to the bid, it should do so in writing or through electronic form that provides record of the content of communication.

### 3. Amendment of Bidding documents

3.1. Before the deadline for submission of bids, the procuring agency for any reason, whether at its own initiative or in response to a clarification requested by a prospective bidder or pre-bid meeting may modify the bidding documents by issuing addendum.

3.2. Any addendum issued including the notice of any extension of the deadline shall be part of the bidding document and shall be uploaded on EPADS v2.0 as well as Authority's website. The procuring agency shall promptly publish the addendum at the procuring agency's website indicated in the **BDS**:

Provided that the bidder who had either already submitted his bid, shall have the right to withdraw his already submitted bid and submit the revised bid, prior to the original or extended bid submission deadline.

3.3. To give prospective bidders reasonable time in which to take an addendum/corrigendum into account in preparing their bids, the Procuring Agency may, at its discretion, extend the deadline for the submission of bids:

Provided that the Procuring Agency shall extend the deadline for submission of bids, if such an addendum is issued within last three (03) days of the bid submission deadline.

## C. Preparation of Bids

### 1. Documents Constituting the Bids

1.1. The bids prepared by the bidders shall constitute the following components: -

1.1.1. Forms of bid and Bid Prices completed in accordance with ITB BDS, GCC and SCC;

1.1.2. Documentary evidence established in accordance with BDS that services to be provided by the bidder are eligible services, and conform to the bidding documents;

1.1.3. Documentary evidence established in accordance with BDS that the bidder is eligible and/or qualified for the subject bidding process;

1.1.4. Documentary evidence established, that the bidder has been authorized to provide the services;

1.1.5. Bid security or Bids Securing Declaration furnished in accordance with BDS; and

1.1.6. Any other document required in the BDS.

### 2. Documents Establishing Eligibility of the Services and Conformity to bidding documents

2.1. To establish the conformity of the Non-Consulting Services to the Bidding document, the bidder shall furnish as part of its bid the documentary evidence that services provided conform to the requirements.

2.2. Standards for the provision of the Non-Consulting Services are intended to be descriptive only and not restrictive.

### 3. Documents Establishing Eligibility and Qualification of the Bidder

3.1. Pursuant to BDS, the bidder shall furnish, as part of its bid, all those documents establishing the bidder's eligibility to participate in the bidding process and/or its qualification to perform the contract if its bid is accepted.

3.2. The documentary evidence of the bidder's eligibility to bids shall establish to the satisfaction of the procuring agency that the bidder, at the time of submission of its bid, is from an eligible country as defined in Section-IV titled as "Eligible Countries".

3.3. The documentary evidence of the bidder's qualifications to perform the contract if its bid is accepted shall establish to the satisfaction of procuring agency that:

3.3.1. the bidder has the financial, technical, and supply/production capability necessary to perform the Contract, meets the qualification criteria specified in BDS.

3.3.2. that the bidder meets the qualification criteria listed in the Bids Data Sheet.

### 4. Form of Bid

**4.1. The bidder shall fill the Form of Bid furnished in the bidding documents. The Bid Forms must be completed without any alterations to its format and no substitute shall be accepted.**

### 5. Bids Prices

5.1. The Bids Prices quoted by the bidder in the Forms of Bid and in the price schedule shall conform to the requirements specified or exclusively mentioned hereafter in the bidding document.

5.2. All items in the Schedule of Requirements must be listed and priced separately in the Price Schedules. If a Price Schedule shows items listed but not priced and neither explicitly mentioned, their prices shall be construed to be included in the prices of other items.

5.3. The Bid price to be quoted in the Forms of Bid shall be the total price of the bid, excluding any discounts offered.

5.4. The bidder shall indicate on the appropriate Price Schedule, the unit prices (where applicable) and total bid price of the services, it proposes to provide under the contract.

5.5. Prices quoted by the bidder shall be fixed during the currency of the contract and not subject to variation on any account. A bid submitted with an adjustable price will be treated as non-responsive and shall be rejected, unless otherwise price adjustment is permissible under Conditions of the Contract. (May be reviewed)

## **6. Price Adjustment**

6.1. Price adjustment shall not be applicable.

6.2. Procuring agency may increase the remuneration of the human resources involved in non-consultancy services on annual basis as per agreement.

**6.3. Procuring agency shall incorporate the provisions to allow wage rate in compliance with Federal Government's minimum wage notification, subject to the applicability in that case.**

## **7. Bids Currencies**

7.1. Prices shall be quoted in Pakistani Rupees unless otherwise specified in the BDS.

## **8. Bid Validity Period**

8.1. Bid(s) shall remain valid for the period specified in the BDS after the bid submission deadline prescribed by the Procuring Agency. A Bid valid for a shorter period shall be rejected by the Procuring Agency as non-responsive. The period of bid validity will be determined from the complementary bid securing instrument i.e. the expiry period of bid security or bid securing declaration as the case may be.

## **9. Bid Security or Bid Securing Declaration**

9.1. Unless otherwise specified in the BDS, the bidder shall furnish as part of its bid, in the amount and currency specified in the BDS or Bid Securing Declaration on the format provided in Section VI (Bid Forms) The scanned copy of the Bids Security shall be uploaded in the EPADS v2.0 while submitting bid, whereas the original forms of Bid Security shall be submitted to the procuring agency before the bid submission deadline. The bidder who failed to submit the original bid security before the submission deadline shall be disqualified straightaway.

9.2. The Bid Security or Bid Securing Declaration is required to protect the Procuring Agency against the risk of Bidder's conduct which would warrant the security's forfeiture.

9.3. The Bid Security shall be payable promptly upon written demand by the Procuring Agency in case any of the conditions listed in BDS, GCC and SCC are invoked.

9.4. Unsuccessful Bidders' Bid Security will be discharged or returned as promptly as possible after the award of contract, however in no case later than thirty (30) days after the expiration of the period of Bid Validity prescribed by the Procuring Agency. The Procuring Agency shall make no claim to the amount of the Bid Security, and shall promptly return the Bid Security document, whichever of the following that occurs earliest:

9.4.1. the expiry of the Bid Security;

9.4.2. the entry into force of a procurement contract and the provision of a Performance Guarantee, for the performance of the contract if such a guarantee, is required by the bidding document;

9.4.3. the rejection by the Procuring Agency of all Bids;

9.4.4. the withdrawal of the Bid prior to the deadline for the submission of bids, unless the bidding document stipulate that no such withdrawal is permitted.

9.5. The Bid Security may be forfeited or the Bid Securing Declaration executed:

9.5.1. if a bidder:

9.5.1.1. withdraws its bid during the period of bid validity as specified by the Procuring Agency, and referred by the bidder in the Forms of Bid, except as provided for in the ITBs; or

9.5.1.2. does not accept the correction of errors, or

9.5.2. in the case of a successful bidder fails:

9.5.2.1. **to sign the contract in accordance with SCC; or**

9.5.2.2. **to furnish Performance Guarantee in accordance with BDS and SCC.**

**9.6. The bid security shall be valid for a period specified in BDS. Bids with shorter bid security validity period shall be rejected straight away.**

## **10. Alternative Bids by Bidders**

10.1. Alternatives will not be considered, unless specifically allowed for in the BDS.

10.2. When alternative times for completion are explicitly invited, a statement to that effect will be included in the BDS and the method of evaluating different time schedules will be described in Evaluation and Qualification Criteria.

## **11. Withdrawal, Substitution, and Modification of Bids**

11.1. Before Bids submission deadline, any bidder may withdraw, substitute, or modify his bid after it has been submitted.

## **12. Format and Signing of Bids**

12.1. The bidder shall prepare and submit his bid with due diligence after carefully reading all the terms and conditions before submission through

EPADS v2.0.

12.2. Any interlineations, erasures, or overwriting shall be valid only if they are signed by the person(s) signing the forms of bid.

## D. Submission of Bids

### 1. Submission of Bids through EPADS v2.0 before Dead deadline

1.1. The Technical and Financial Bids as the case may be, shall be submitted in the due portion of the EPADS v2.0, before bid submission deadline. The bid submission option shall be automatically disabled once the deadline is over.

1.2. The Procuring Agency may, under exceptional circumstances and at its discretion, extend the deadline for the submission of bids by amending the Bidding Documents. In such a case, all rights and obligations of the Procuring Agency and the Bidders that were previously subject to the original deadline shall thereafter be subject to the revised deadline.

## E. Opening and Evaluation of Bids

### 1. Opening & Evaluation of Bids by the Procurement Cell/Evaluation Committee

1.1. The Procuring Agency is to constitute an odd number Bid Evaluation Committee for the purpose of bid opening and evaluation of all procurements. As per Rules 29 & 30 of Public Procurement Rules, 2004, The Procuring Agency is required to establish a Procurement Cell/Evaluation Committee which shall evaluate the Bids in accordance with the evaluation criteria, terms and conditions given in the bidding documents.

1.2. The selection technique adopted shall be based on quality and cost, with 70% weightage assigned to quality and 30% to cost. The passing threshold for the technical bid shall be 70%.

### 2. Opening of Bids

2.1. The Bid Evaluation Committee of the Procuring Agency will open all bids through EPADS, in the presence of bidders' or their representatives who choose to attend, and other parties with a legitimate interest in the bid proceedings at the place, on the date and at the time, specified in the **BDS**. The Bidders' representatives present shall sign attendance sheet as proof of their attendance.

2.2. The bids shall be opened one at a time, and the following read out and recorded: (a) the name of the bidder; (c) the presence of a bid security, if required; and (d) any other details as the procuring agency may consider appropriate.

2.3. No bid will be rejected at the time of bid opening except for bids whose bid security has not been provided to the procuring agency before submission deadline.

2.4. The procuring agency shall prepare minutes of the bid opening. The record of the bid opening shall include, as a minimum: the name of the bidder and the bid price, if applicable.

### 3. Confidentiality

3.1. Information relating to the examination, clarification, evaluation and comparison of bids and recommendation of contract award shall not be disclosed to bidders or any other person(s) not officially concerned with such process, until the time of the announcement of the respective evaluation report.

3.2. Any effort by a bidder to influence the procuring agency processing of bids or award decision may result in the rejection of his bid.

### 4. Preliminary Examination of Bids

4.1. Prior to the detailed evaluation of bids, the procuring agency will determine whether each bid:

4.1.1. meets the eligibility criteria defined in **BDS**;

4.1.2. has been prepared as per the format and contents defined by the procuring agency in the bidding document;

4.1.3. is accompanied by the required securities; and

4.1.4. is substantially responsive to the requirements of the bidding document.

4.2. The procuring agency will confirm that the documents and information specified under **BDS, GCC and SC** have been provided in the bids. If any of these documents or information is missing, or is not provided in accordance with the Instructions to Bidders, the bids shall be rejected.

4.3. If a bid is not substantially responsive, it will be rejected by the procuring agency and may not subsequently be evaluated for complete technical responsiveness.

## 5. Examination of Terms and Conditions, Technical Evaluation

5.1. The procuring agency shall evaluate the technical aspects of the bids submitted in accordance with **BDS**, to confirm that all requirements specified in **Evaluation Criteria, Technical Specifications and Schedule of Requirements**, prescribed in the bidding document have been met without material deviation or reservation.

5.2. If after the examination of the terms and conditions and the technical evaluation, the procuring agency determines that the bid is not substantially responsive in accordance with **BDS**, it shall reject the bids.

## 6. Correction of Errors

6.1. Bids determined to be substantially responsive will be checked for any arithmetic errors. Errors will be corrected as follows: -

6.1.1. if there is a discrepancy between unit prices and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected, unless in the opinion of the procuring agency there is an obvious misplacement of the decimal point

in the unit price, in which the total price as quoted shall govern and the unit price shall be corrected;

6.1.2. if there is an error in a total corresponding to the addition or subtraction of sub-totals, the sub-totals shall prevail and the total shall be corrected; and

6.1.3. where there is a discrepancy between the amounts in figures and in words, the amount in words will govern.

6.1.4. Where there is discrepancy between grand total of price schedule and amount mentioned on the Forms of bid, the amount referred in Price Schedule shall be treated as correct subject to elimination of other errors.

6.2. The amount stated in the bid will be adjusted by the procuring agency in accordance with the above procedure for the correction of errors and, with the concurrence of the bidder that shall be considered as binding upon the bidder. If the Bidder does not accept the corrected amount, his bid will then be rejected, and the Bid Security may be forfeited or the Bid Securing Declaration may be executed.

## **7. Conversion to Single Currency**

7.1. As per Rule 30 of Public Procurement Rules, 2004.

## **8. Evaluation of Bids**

8.1. The procuring agency shall evaluate bids in accordance with Rule 30 of Public Procurement Rules, 2004 and compare only those bids determined to be substantially responsive.

8.2. In evaluating the Technical Bids of each Bidder, the Procuring Agency shall apply the evaluation criteria and methodologies specified in the Bid Data Sheet (BDS) and in accordance with the Statement of Requirements and Technical Specifications. No other evaluation criteria or methodologies shall be permitted.

8.3. In case of tie of bids, the bidders shall be provided an opportunity to offer their best and final monetary offer through EPADS. However, in no case

the rates shall be higher than the original financial bids.

8.4. The Procuring agency evaluation of a bid will take into account:

8.4.1. the bid price, excluding provisional sums and the provision, if any, for contingencies in the summary bill of quantities, but including day work items, where priced competitively;

8.4.2. price adjustment for correction of arithmetic errors in accordance with **ITB 6**;

8.5. converting the amount resulting from applying (a) and (b) above, if relevant, to a single currency in accordance with **ITB 7**;

8.6. The estimated effect of the price adjustment provisions of the Conditions of Contract, applied over the period of execution of the Contract, shall not be taken into account in bid evaluation.

8.7. If these bidding documents allow bidders to quote separate prices for different lots, and the award to a successful bidder of multiple lots, the methodology of evaluation to determine the lowest evaluated lot combinations in the Form of Bid, is specified in the **BDS**.

## 9. **Determination of Most Advantageous Bids**

9.1. Selection technique will be adopted for determining the Successful Bid in accordance with the criteria referred in the **BDS** or prescribed in the separate section titled as Evaluation Criteria.

## 10. **Abnormally Low Financial Bids**

10.1. Procuring agency may reject a bid if it has determined that the price, in combination with other constituent elements of the bid, is abnormally low in relation to the subject matter of the procurement, such that it raises material concerns on the part of the procuring agency, as to the ability of the bidder to perform the procurement contract satisfactorily for the offered price.

A procuring agency shall not reject a bid as abnormally low under sub-clause (1) above unless the procuring agency -

10.1.1. requested in writing through EPADS from the bidder a written clarification of his bid, including a detailed price analysis of his bid price in relation to the subject matter of the procurement contract, scope, methodology, schedule, allocation of risks and responsibilities and any other requirements of the bidding document; and

10.1.2. having taken account, the information provided by the bidder in response to a request under paragraph (a) and the information included in the bid, the procuring agency determines that the bidder has failed to demonstrate its ability to perform the procurement contract satisfactorily for the offered price.

The procuring agency shall promptly communicate to the bidder concerned its decision to reject the bid, including the reasons for the decision.

## **11. Rejection of Bids**

11.1. As per Rule 33 of the Public Procurement Rules, 2004

## **12. Single Responsive Bid**

12.1. The procuring agency may consider single responsive bid subject to underlying conditions of Rule 38(b) of the Public Procurement Rules, 2004.

## **13. Arbitration**

13.1. As per Rule 49 of Public Procurement Rules, 2004.

# **F. Award of Contract**

## **1. Criteria of Award**

1.1. The procuring agency will award the Contract to the bidder whose bid has been determined to be substantially responsive to the bidding document and who has been declared as most advantageous Bid.

## 2. Procuring Agency's Right to reject All Bids

2.1. The procuring agency reserves the right to reject all the Bids and to annul the procurement process at any time prior to acceptance of the bid(s), without thereby incurring any liability to the affected bidder(s).

2.2. Notice of the rejection of all bids shall be given promptly to all bidders that have submitted the bids. The procuring agency shall upon request communicate to any bidder the grounds for the rejection of his bid, but is not required to justify those grounds.

## 3. Notification of Award

3.1. Prior to the award of contract, the procuring agency shall issue a Final Evaluation Report giving justification for acceptance or rejection of the bids.

3.2. Bidder whose bid has been accepted, will be notified for the award by the Procuring Agency prior to expiration of the Bid Validity period through EPADS. The Letter of Acceptance will state the sum that the procuring agency will pay the successful bidder in consideration for the execution of the scope of works as prescribed by the Contract (hereinafter and in the Contract called the "Contract Price).

3.3. The notification of award will constitute the formation of the Contract, subject to the condition that bidder furnish the Performance Guarantee and signing of the contract.

## 4. Signing of Contract

4.1. Promptly after notification of award, Procuring Agency shall send the successful bidder the draft agreement, incorporating all terms and conditions as agreed by the parties to the contract. The successful bidder and the procuring agency shall sign the contract.

## 5. Performance Guarantee

5.1. After the receipt of the Letter of Acceptance, the successful bidder, within the specified time, shall deliver to the Procuring Agency a Performance Guarantee in the amount and in the form stipulated in the **BDS**

**and SCC**, denominated in the type and proportions of currencies in the Letter of Acceptance and in accordance with the Conditions of Contract.

5.2. Failure of the successful bidder to comply with the requirement of **BDS, SCC and GCC** shall constitute sufficient grounds for the annulment of the award and forfeiture of the bid security, in which event the procuring agency may make the award to the next ranked bidder or call for new bids.

## **6. Corrupt & Fraudulent Practices**

6.1. Procuring Agencies (including beneficiaries of Government funded projects and procurement) as well as Bidders/Contractors under Government financed contracts, observe the highest standard of ethics during the procurement and execution of such contracts, and will avoid to engage in any corrupt and fraudulent practices.

## **G. Grievance Redressal & Complaint Review Mechanism**

### **1. Constitution of Grievance Redressal**

1.1. Procuring agency shall constitute a Grievance Redressal Committee (GRC) comprising of an odd number of persons with proper power and authorization to address the complaint. The GRC shall not have any of the members of Procurement Evaluation Committee.

### **2. GRC Procedure**

2.1. Any aggrieved party or bidder as the case may be, may file grievance in accordance with Rule 48 of the Public Procurement Rules, 2004 and Redressal of Grievance Regulations, 2022

## **H. Blacklisting/ Debarment**

### **1. Procedure for Blacklisting/Debarment**

1.1. The procuring agency may initiate blacklisting proceedings against contractor/supplier in accordance with Rule-19of the Public Procurement

Rules, 2004, Mechanism for Blacklisting, Debarment Regulations, 2024 and Regulation on "procedure for filing and disposal of review petition under rule-19(3) of the Public Procurement Rules, 2004.





## Bid Data Sheet

# Bids Data Sheet (BDS)

The following specific data for the procurement of Goods to be procured shall complement, supplement, or amend the provisions in the Instructions to Bidders (ITB). Whenever there is a conflict, the provisions herein shall prevail over those in ITB.

## **BDS Clause Number**

### **ITB Number**

## **Amendments of, and Supplements to, Clauses in the Instruction to Bidders**

### **A. Introduction**

#### **BDS Clause Number 1**

Name of Procuring Agency: **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce)**

The subject of procurement is: **OGDCL Cyber Risk Reinsurance Coverage**

Expected commencement date: **Monday, August 3, 2026**

#### **BDS Clause Number 2**

Financial year for the operations of the Procuring Agency: **2026-27**

Name and identification number of the Contract: **P44738**

#### **BDS Clause Number 3**

JV/Consortium or Association Allowed: **No**

Number of JV/Consortium Members: **Nil**

### **B. Bidding Documents**

#### **BDS Clause Number 4**

The Bidders may seek clarifications through **EPADS v2.0**: Clarification Date: Thursday, July 2, 2026

#### **BDS Clause Number 5**

Any addendum, in case issued, shall be published on **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce)** website and on **EPADS**

**v2.0.**

**BDS Clause Number 6**

List of documents required along with the bid: No

**BDS Clause Number 7**

The qualification criteria to establish the supply / production capability of the bidder.

*see Eligibility Criteria*

**BDS Clause Number 8**

**Services and Their related documents:**

*See section Required Services and Scope of Work*

**BDS Clause Number 9**

Price schedule will be provided according to the format defined and acquired.

*see section price schedule.*

**BDS Clause Number 10**

**Specifications:**

*see section of specifications.*

**C. Preparation of Bids**

**BDS Clause Number 11**

The price shall be **Fixed**.

**BDS Clause Number 12**

Currency of the Bids shall be : **PKR**

**BDS Clause Number 13**

The Bids/Bid Validity period shall be: **45 Days**

**BDS Clause Number 14**

The amount of Bid Security shall be as defined in Bid Security Section for items and lots given in **BDS 6**

The Bid Security shall be in the form of: **Pay Order, Bank Guarantee, Others**

### **BDS Clause Number 15**

The Bids security shall be valid for twenty-eight (28) days beyond the expiry of the Bids validity period specified in the bidding documents, for example the bid validity is 90days so the bid security shall be valid for  $90+28 = 118$  days.

### **BDS Clause Number 16**

Alternative Bids to the requirements of the bidding documents willnot be permitted.

## **D. Submission of Bids**

### **BDS Clause Number 17**

Bid shall be submitted online on EPADS v2.0 whereas hard copy of the bid security should be submitted to the following;

**PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).**

Bids that are not submitted on EPADS v2.0 shall be disqualified.

The deadline for Bids submission is: **Tuesday, July 7, 2026 11:00 AM**

## **E. Opening and Evaluation of Bids**

### **BDS Clause Number 18**

The Bids opening shall take place on **EPADS v2.0**.

Day : **Tuesday**

Date: **Tuesday, July 7, 2026**

Time : **11:30 AM**

### **BDS Clause Number 19**

Selection technique adopted will be: **Least Cost Based Selection (LCBS)**  
*see Evaluation Criteria*

## **F. Award of Contract**

### **BDS Clause Number 20**

The Performance guarantee shall: **0%**.

The Performance Guarantee shall be acceptable in the form of:**Nil**

**21.**

**51.1**

Arbitrator shall be appointed by mutual consent of the both parties.

## G. Review of Procurement Decisions

### **BDS Clause Number 22**

Grievance against this procurement shall be submitted online on EPADS v2.0.



## Eligibility Criteria

| Bidder's Type                  | Required Registration |
|--------------------------------|-----------------------|
| Partnership Firm               | None                  |
| Company (Private Limited)      |                       |
| Company (Public Limited)       |                       |
| Company (Holding Company)      |                       |
| Company (Limited by Guarantee) |                       |

| Eligibility Criteria  | Document |
|---|----------|
| The bidder should be an international (re)insurance broker having an annual premium placement volume of at least USD 500 million.               | Yes      |
| Bidder(s) must affirm that they are not blacklisted by any Government, Semi-Government, or Autonomous body within the jurisdiction of Pakistan. | Yes      |
| Bidder(s) are required to submit a duly signed Integrity Pact for contracts valuing PKR 10 million and above.                                   | Yes      |

## Evaluation Criteria

### Least Cost Based Selection (LCBS)

| Technical Marks   | 100 |
|---|-----|
| Passing Marks   | 100 |
| Regulatory Compliance   |     |
| Foreign brokers as well as local affiliates to submit valid professional indemnity policies meeting regulatory requirements of their respective countries of registration. (Quantitative)(Doc Required) | 5   |
| Lead Reinsurer Information  |     |
| Name of Lead Reinsurer (Quantitative)(Doc Required)   | 5   |
| Lead Reinsurer Rating: minimum "A" as per S&P/AM Best Moody's and Fitch (Quantitative)(Doc Required)  | 10  |
| Lead Reinsurer Share: at least 15%, not more than 25% (Quantitative)(Doc Required)  | 5   |
| Country of Origin (Quantitative)(Doc Required)  | 5   |
| Bidder must abide by the following:   |     |
| The quotation should be "FIRM" quote (Quantitative)(Doc Required)   | 5   |
| Validity of quote should be 45 days from date of opening of bid (Quantitative)(Doc Required)  | 10  |
| No underwriting agencies are allowed as leader (Quantitative)(Doc Required)   | 10  |
| Quotation/slip/policy wording should be without any expressed or implied subjectivities/conditions/additional exclusions/warranties (Quantitative)(Doc Required)  | 5   |
| Premium Payment warranty should be ninety (90) days from the inception of the policy period. (Quantitative)(Doc Required)   | 5   |
| Law and Jurisdiction must be Pakistan (Quantitative)(Doc Required)  | 5   |
| Actual Quotation slip/policy wording signed/stamped by the leader must be attached. (Quantitative)(Doc Required)  | 10  |

|   |    |
|---|----|
| Limit of Liability  |    |
| USD 10,000,000 each and every claim and in the aggregate including costs and expenses. The overall Aggregate limit of indemnity for all Insuring Clauses is USD 10,000,000 (Quantitative)(Doc Required) | 10 |
| Deductibles   |    |
| USD 250,000 each and every claim Network Interruption Loss Waiting Hours: 12 Hours Reputational Harm: 14 Days (Quantitative)(Doc Required)  | 10 |

## Required Services

### Positions Without Lots :

| Position  | Delivery Schedule   | Quantity | Bid Security |
|---|---|----------|--------------|
| OGDC Cyber Risk Cover<br>(Net to Broker in PKR) | <p><b>Address:</b> PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).</p> <p><b>Schedule:</b> as per work order <b>Quantity:</b> 1</p> | 1        | 120000       |

### Related Services :

No

### Services Specifications

**Positions Without Lots :**

**Position:** OGDC Cyber Risk Cover (Net to Broker in PKR)

**Specifications / Requirements:**

as per attached annexures

**Scope of Work**

as per attached annexures

**Price Schedule**

**For Individual Positions**

| # | Position Title | Quantity | Unit Price (PKR) | Total Price (PKR) | Delivery Location | Delivery Period / Year | Country of Origin |
|---|----------------|----------|------------------|-------------------|-------------------|------------------------|-------------------|
| 1 |                |          |                  |                   |                   |                        |                   |
| 2 |                |          |                  |                   |                   |                        |                   |

**For Lots**

| # | Lot Title     | Total Lot Price (PKR) | Country of Origin |
|---|---------------|-----------------------|-------------------|
| 1 | [Lot 1 Title] |                       |                   |





## General Conditions of Contract

## A. General

### 1. Definitions

1.1. Unless the context otherwise requires, the following terms whenever used in this Contract shall have the same meaning and shall be interpreted as indicated

1.1.1. "Applicable Law" means the laws and any other instruments having the force of law in the Government's Country, or in such other country as may be specified in the Special Conditions of the Contract (SC), as they may be issued and in force from time to time;

1.1.2. "The Contract" means an agreement enforceable by law;

1.1.3. "The Contract Price" means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations;

1.1.4. "The Services" means the work to be performed by the Contractor pursuant to this Contract and as prescribed in the Specifications and Schedule of Activities included in the Contractor's Bid;

1.1.5. "Ancillary Services" means those services ancillary to the provision of Services, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, training, and other such obligations of the Contractor covered under the Contract;

1.1.6. "GCC" means the General Conditions of Contract contained in this section;

1.1.7. "SCC" means the Special Conditions of Contract by which the GCC may be amended or supplemented;

1.1.8. "Day" means calendar day unless indicated otherwise;

1.1.9. "Effective Date" means the date on which this Contract comes into force and effect;

1.1.10. "The Contractor" means the individual or corporate body whose Bids to provide the Services has been accepted by the Procuring Agency;

1.1.11. "The Project Site," where applicable, means the place or places named in Bid Data Sheet and technical Specifications;

1.1.12. "Government" means the Government of Pakistan;

1.1.13. "Local Currency" means the currency of Pakistan;

1.1.14. "In Writing" means communicated in written form with proof of receipt;

1.1.15. "Completion Date" means the date of completion of the Services by the Contractor as certified by the Procuring Agency;

1.1.16. "Foreign Currency" means any currency other than the currency of the country of the Procuring Agency;

1.1.17. "Party" means the Procuring Agency or the Contractor, as the case may be, and "Parties" means both of them;

1.1.18. "Service" means any object of procurement other than goods or works;

1.1.19. "Subcontractor" means any entity to which the Bidder subcontracts any part of the Services.

## 2. **Applicable Law**

2.1. The contract shall be governed and interpreted in accordance with the laws of Pakistan, unless otherwise specified in SCC.

## 3. **Language**

3.1. The Contract as well as all correspondence and documents relating to the Contract exchanged between the Contractor and the Procuring Agency, shall be written in the **English language** unless otherwise stated in the SCC. Supporting documents and printed literature that are part of the Contract may be in another language provided these are accompanied by an accurate translation of the relevant passages in English, in which case, for purposes of interpretation of the Contract, this translation shall govern.

## 4. **Notices**

4.1. Any notice, request, or consent made pursuant to this Contract shall be in writing and shall be deemed to have been made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram, or facsimile to such Party at the address specified in the SCC.

## 5. **Location**

5.1. The Services shall be performed at such locations as the Procuring Agency may approve and as specified in SCC.

## 6. **Authorized Representatives / Authority of Member in charge**

6.1. Any action required or permitted to be taken, and any document required or permitted to be executed, under this Contract by the Procuring Agency or the Contractor may be taken or executed by the officials specified in the SCC.

# B. **Commencement, Completion, Modification, and Termination of Contract**

## 1. **Effectiveness of Contract**

1.1. This Contract shall come into effect on the date the Contract is signed by both parties and such other later date as may be stated in the SCC.

## 2. Commencement of Services

2.1. The Contractor shall confirm availability of Key Experts and begin carrying out the Services not later than the number of days after the Effective Date specified in the SCC.

## 3. Program schedule

3.1. Before commencement of the Services, the Contractor shall submit to the Procuring Agency for approval a Program showing the general methods, arrangements, order and timing for all activities. The Services shall be carried out in accordance with the approved Program as updated.

## 4. Starting Date/Expiration Date

4.1. The Contractor shall start carrying out the Services Five (05) days after the date the Contract becomes effective, or at such other date as may be specified in the SCC.

4.2. Unless terminated earlier pursuant to Clause **GCC 14** hereof, this Contract shall expire at the end of such time period after the Effective Date as specified in the SCC.

## 5. Entire Agreement

5.1. This Contract contains all covenants, stipulations and provisions agreed by the Parties. No agent or representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.

## 6. Modification

6.1. Any modification or variation of the terms and conditions of this Contract, including any modification or variation of the scope of the Services, may only be made by written agreement between the Parties. However, each Party shall give due consideration to any modification(s) or variation(s) made by the other Party.

6.2. In cases of any modification(s) or variation(s), the prior written consent of the Procuring Agency is required.

## 7. Force Majeure

### 7.1. Definition

For the purposes of this Contract, "Force Majeure" means an event which is beyond the reasonable control of a Contractor and which makes a Contractor's performance of its obligations under the Contract impossible or so impractical as to be considered impossible under the circumstances.

### 7.2. No Breach of Contract

The failure of a Party to fulfill any of its obligations under the contract shall not be considered to be a breach of, or default under, this Contract in so far as such inability arises from an event of Force Majeure, provided that the Party affected by such an event (a) has taken all reasonable precautions, due care and reasonable alternative measures in order to carry out the terms and conditions of this Contract, and (b) has informed the other Party as soon as possible about the occurrence of such an event.

### 7.3. Extension of Time

Any period within which a Contractor shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

### 7.4. Payments

During the period of their inability to perform the Services as a result of an event of Force Majeure, the Contractor shall be entitled to continue to be paid under the terms of this Contract, as well as to be reimbursed for additional costs reasonably and necessarily incurred by them during such period for the purposes of the Services and in reactivating the Service after the end of such period.

## 8. Termination

### 8.1. By the Procuring Agency

The Procuring Agency may terminate this Contract in case of the occurrence of any of the events specified in paragraphs (a) through (e) of this Clause. In such an occurrence the Procuring Agency shall give at least thirty (30) calendar days' written notice of termination to the Contractor in case of the events referred to in (a) through (d); at least sixty (60) calendar days' written notice in case of the event referred to in (e);

8.1.1. If the Contractor fails to remedy a failure in the performance of its obligations hereunder, as specified in a notice of suspension;

8.1.2. If the Contractor becomes (or, if the Contractor consists of more than one entity, if any of its members becomes) insolvent or bankrupt or enter into any agreements with their creditors for relief of debt or take advantage of any law for the benefit of debtors or go into liquidation or receivership whether compulsory or voluntary;

8.1.3. If the Contractor fails to comply with any final decision reached as a result of arbitration proceedings;

8.1.4. If, as the result of Force Majeure, the Contractor is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days;

8.1.5. If the Procuring Agency, in its sole discretion and for any reason whatsoever, decides to terminate this Contract;

### 8.2. By the Contractor

The Contractor may terminate this Contract, by not less than thirty (30) calendar days' written notice to the Procuring Agency, in case of the occurrence of any of the events specified in paragraphs (a) through (d) of this Clause.

8.2.1. If the Procuring Agency fails to pay any money due to the Contractor pursuant to this Contract and not subject to dispute within forty-five (45) calendar days after receiving written notice from the Contractor that such payment is overdue;

8.2.2. If, as the result of Force Majeure, the Contractor is unable to perform a material portion of the Services for a period of not less than sixty (60) calendar days;

8.2.3. If the Procuring Agency fails to comply with any final decision reached as a result of arbitration;

8.2.4. If the Procuring Agency is in material breach of its obligations pursuant to this Contract and has not remedied the same within forty-five (45) days (or such longer period as the Bidder may have subsequently approved in writing) following the receipt by the Procuring Agency of the Contractor's notice specifying such breach.

## C. Obligations of the Contractor

### 1. General

#### 1.1. Standard of Performance

1.1.1. The Contractor shall perform the Services and carry out the Services with all due diligence, efficiency and economy, in accordance with generally accepted professional standards and practices, and shall observe sound management practices, and employ appropriate technology and safe and effective equipment, machinery, materials and methods. The Contractor shall always act, in respect of any matter relating to this Contract or to the Services, as a faithful adviser to the Procuring Agency, and shall at all times support and safeguard the Procuring Agency's legitimate interests in any dealings with the third parties;

1.1.2. The Contractor shall employ and provide such qualified and experienced Experts and Sub-Contractors as are required to carry out the Services.

#### 1.2. Law Applicable to Services

The Contractor shall perform the Services in accordance with the Contract and in accordance with the Law of Pakistan and shall take all practicable steps to ensure that any of its Experts and Sub-Bidders, comply with the Applicable Law.

### 2. Conflict of Interests

#### 2.1. Contractor Not to Benefit from Commissions and Discounts

The remuneration of the Contractor shall constitute the Contractor's sole remuneration in connection with this Contract or the Services, and the Contractor shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Contractor shall use their best efforts to ensure that the Personnel, any Subcontractors, and agents of either of them similarly shall not receive any such additional remuneration.

#### 2.2. Contractor and Affiliates Not to be Otherwise Interested in Project

The Contractor agree that, during the term of this Contract and after its termination, the Contractor and its affiliates, as well as any Subcontractor and any of its affiliates, shall be disqualified from providing Services (other than the Services and any continuation thereof) for any project resulting from or closely related to the Services.

#### 2.3. Prohibition of Conflicting Activities

Neither the Bidder nor its Subcontractors nor the Personnel shall engage, either directly or indirectly, in any of the following activities:

2.3.1. during the term of this Contract, any business or professional activities in the Government's country which would conflict with the activities assigned to them under this Contract;

2.3.2. during the term of this Contract, neither the Contractor nor their Subcontractors shall hire public employees in active duty or on any type of leave, to perform any activity under this Contract;

2.3.3. after the termination of this Contract, such other activities as may be specified in the SCC.

### **3. Insurance to be Taken Out by the Contractor**

3.1. The Contractor(a) shall take out and maintain, and shall cause any Subcontractors to take out and maintain, at its (or the Sub-contractors', as the case may be) own cost but on terms and conditions approved by the Procuring Agency, insurance against the risks, and for the coverage, as shall be specified in the SCC; and (b) at the Procuring Agency's request, shall provide evidence to the Procuring Agency showing that such insurance has been taken out and maintained and that the current premiums have been paid.

### **4. Contractor's Actions Requiring Procuring Agency's Prior Approval**

4.1. The Contractor shall obtain the Procuring Agency's prior approval in writing before taking any of the following actions:

4.1.1. appointing such members of the Personnel not provided by the Contractor;

4.1.2. changing the Program of activities; and

4.1.3. any other action that may be specified in the SCC.

### **5. Reporting Obligations**

5.1. The Contractor shall submit to the Procuring Agency the reports and documents in the numbers, and within the periods as prescribed by the Procuring Agency.

### **6. Liquidated Damages**

#### **6.1. Payments of Liquidated Damages**

The Contractor shall pay liquidated damages to the Procuring Agency at the rate per day stated in the SCC for each day that the Completion Date is later than the Intended Completion Date. The total amount of liquidated damages shall not exceed the amount defined in the SCC. The Procuring Agency may deduct liquidated damages from payments due to the Contractor. Payment of liquidated damages shall not affect the Contractor's liabilities.

#### **6.2. Correction for Over-payment**

If the Intended Completion Date is extended after liquidated damages have been paid, the Procuring Agency shall correct any overpayment of liquidated damages by the Contractor by adjusting the next payment certificate. The Contractor shall be paid interest on the overpayment, calculated from the date of payment to the date of repayment, at the rates specified in SCC.

### 6.3. Lack of performance penalty

If the Contractor has not corrected a Defect within the time specified in the Procuring Agency's notice, a penalty for Lack of performance will be paid by the Contractor. The amount to be paid will be calculated as a percentage of the cost of having the Defect corrected, assessed as specified in the Contractor

## 7. Performance Guarantee

7.1. Within the time stipulated in the acceptance letter from the Procuring Agency, the successful Bidder shall furnish the Performance Guarantee in shape and amount **specified in SCC**.

7.2. The proceeds of the Performance Guarantee shall be payable to the Procuring agency as compensation for any loss resulting from the Supplier's failure to complete its obligations under the Contract.

7.3. The Performance Guarantee shall be denominated in the currency of the Contract, or in a freely convertible currency acceptable to the Procuring agency and shall be in the acceptable form as specified in **SCC**.

7.4. The Performance Guarantee will be discharged by the Procuring agency and returned to the Supplier not later than thirty (30) days following the date of completion of the Supplier's performance obligations under the Contract, including any warranty obligations, unless otherwise **specified in SCC**.

## 8. Sustainable Procurement

8.1. The Contractor shall conform to the sustainable procurement contractual provisions, if and as specified in the **SCC**.

## D. Contractor's Personnel

### 1. Description of Personnel

1.1. The titles, agreed job descriptions, minimum qualifications, and estimated periods of engagement in the carrying out of the Services of the Contractor's Key Personnel. The Key Personnel listed by title as well as by name are hereby approved by the Procuring Agency.

### 2. Removal and / or Replacement of Personnel

2.1. Except as the Procuring Agency may otherwise agree, no changes shall be made in the Key Personnel. If, for any reason beyond the reasonable control of the Contractor, it becomes necessary to replace any of the Key Personnel, the Contractor shall provide as a replacement a person of equivalent or better qualifications.

2.2. If the Procuring Agency finds that any of the Personnel have (i) committed serious misconduct or have been charged with having committed a criminal action, or (ii) have reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Contractor shall, at the Procuring Agency's written request specifying the grounds thereof, provide as a replacement a person with qualifications and experience acceptable to the Procuring Agency.

2.3. The Contractor shall have no claim for additional costs arising out of or incidental to any removal and/or replacement of Personnel.

## E. Obligations of the Procuring Agency

### 1. Change in the Applicable Law

1.1. If, after the date of this Contract, there is any change in the Applicable Law with respect to taxes and duties which increases or decreases the cost of the Services rendered by the Contractor, then the remuneration and reimbursable expenses otherwise payable to the Contractor under this Contract shall be increased or decreased accordingly by agreement between the Parties, and corresponding adjustments shall be made to the amounts referred in the SCC.

### 2. Services and Facilities

2.1. The Procuring Agency shall make available to the Contractor and the Experts, for the purposes of the Services and free of any charge, the services, facilities and property described in the Terms of Reference, at the times and in the manner specified in the Terms of Reference.

2.2. In case that such services, facilities and property shall not be made available to the Contractor, the Parties shall agree on (i) any time extension that it may be appropriate to grant to the Contractor for the performance of the Services, (ii) the manner in which the Contractor shall procure any such services, facilities and property from other sources, and (iii) the additional payments, if any, to be made to the Contractor as a result thereof.

## F. Payments to the Contractor

### 1. Contract Price

1.1. The price payable shall be in Pakistani Rupees unless otherwise specified in the SCC.

### 2. Terms and Conditions of Payment

2.1. Payments will be made to the Contractor according to the payment schedule stated in the SCC and as per actual invoice submitted by the Contractor.

2.2. Unless otherwise stated in the SCC, the advance payment shall be made against the provision by the Contractor of a bank guarantee for the same amount, and shall be valid for the period stated in the SCC. Any other payment shall be made after the conditions listed in the SCC for such payment have been met, and the Contractor have submitted an invoice to the Procuring Agency specifying the amount due.

### 3. Quality Control Identifying Defects

3.1. The principle and modalities of Inspection of the Services by the Procuring Agency shall be as indicated in the SCC. The Procuring Agency shall check the Contractor's performance and notify him of any Defects that are found. Such checking shall not affect the Contractor's responsibilities. The Procuring Agency may instruct the Contractor to search for a Defect and to uncover and test any service that the Procuring Agency considers may have a Defect. Defect Liability Period is as defined in the SCC.

### 4. Correction of Defects, and Lack of Performance Penalty

4.1. The Procuring Agency shall give notice to the contractor of any Defects before the end of the Contract. The Defects liability period shall be extended for as long as Defects remain to be corrected.

4.2. Every time notice a Defect is given; the contractor shall correct the notified Defect within the length of time specified by the Procuring Agency's notice.

4.3. If the contractor has not corrected a Defect within the time specified in the Procuring Agency's notice, the Procuring Agency will assess the cost of having the Defect corrected, the contractor will pay this amount, and a Penalty for Lack of Performance.

## 5. Settlement of Disputes Amicable Settlement

5.1. The Parties shall use their best efforts to settle amicably all disputes arising out of or in connection with this Contract or its interpretation.

## 6. Dispute Settlement

### 6.1. Arbitration

If any dispute of any kind whatsoever shall arise between the procuring agency and the contractor in connection with or arising out of the Contract, including without prejudice to the generality of the foregoing, any question regarding its existence, validity or termination, or the execution of the contract, the parties shall seek to resolve any such dispute or difference by mutual consultation. If the parties fail to resolve such a dispute or difference even after negotiations or mediation, then the dispute shall be referred within fourteen (14) days in writing by either party to the Arbitrator, with a copy to the other party.

Any dispute in respect of which a notice of intention to commence arbitration has been given, in accordance with **GCC sub-clause 32.1**, shall be finally settled by arbitration. Arbitration may be commenced prior to or after completion of the Contract. Arbitration proceedings shall be conducted in accordance with Arbitration Act 1940. Notwithstanding any reference to arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless otherwise agreed. The Procuring Agency shall continue to pay the Contractor any undisputed amounts due under the Contract during the resolution of any dispute.



## Special Conditions of Contract

## SECTION VIII. SPECIAL CONDITIONS OF CONTRACT

The following Special Conditions of Contract shall supplement the General Conditions of Contract. Whenever there is a conflict, the provisions herein shall prevail over those in the Conditions of Contract. The corresponding clause number of the GCC is indicated in parentheses.

### Number of GC Clause

### Amendments of, and Supplements to, Clauses in the General Conditions of Contract

### Definitions

**The Procuring Agency is:** Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).

### The Supplier is:

**The title of the subject procurement is:** OGDCL Cyber Risk Reinsurance Coverage

### Number of GC Clause 2

### Applicable/Governing Law:

The Contract shall be interpreted in accordance with the laws of Islamic Republic of Pakistan

### Number of GC Clause 3

### Language:

The language of the Contract, all correspondence and communications to be given, and all other documentation to be prepared and supplied under the Contract shall be in **English**.

### Number of GC Clause 4

### Notices:

### The addresses for the notices are:

Procuring Agency:

Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).

+92-300-699-8576

aghafoor@pakre.org.pk

Contractor/ Bidder:

[Name, address and telephone number].

The Contractor/ Bidder's Representative(s)

[Name, address, telephone number and e-mail address]

**Number of GC Clause 6.1**

**The Authorized Representatives are:**

**For the Procuring Agency:**

Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist  
PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District),  
Karachi (Division), Sindh (Province).  
+92-300-699-8576  
aghafoor@pakre.org.pk

**For the Bidder:**

**Name:** .....

**Designation:** .....

**Address:** .....

**Number of GC Clause 7**

**Effectiveness of the contract**

The Contractor/Bidder shall be effective within ..... days from the date of signature of the Contract by both parties

**Number of GC Clause 8**

**Commencement of Contract:**

The Contractor/ Bidder shall provide Non-Consultancy Services from the effective date of contract.

**Number of GC Clause 10.2**

**Expiration of Contract:**

The time period shall be .....

**Number of GC Clause 14**

**Termination**

In the event of termination of the contract due to any reason as already defined in the General Conditions of Contract, the Bidder shall be responsible for providing to the Authority the Service still the time of alternate arrangements.

**Number of GC Clause 16**

**Conflict of Interest:**

The Procuring Agency reserves the right to determine on a case-by-case basis whether the Bidder should be disqualified from providing services due to a conflict of a nature described in Clause GCC C2.

**Number of GC Clause 20**

## **Liquidated Damages**

If the Bidder fails to provide services as required under the contract or in case of any data loss/data breach or any incident compromising the data security or other such failures related to any services, the Bidder shall pay to the Procuring Agency as Liquidated Damages at a rate of **0.01%** to **10.00%** of the Contract value, in accordance with the extent of performance failure & the cost of investigating such incidents as judged by the Authority.

## **Number of GC Clause 21**

### **Performance Guarantee:**

The amount of performance guarantee shall be 0% of the contract price in acceptable form of Nil

## **Number of GC Clause 27**

### **Currency of Payment:**

All the payment to be released to the contractor/Bidder shall be in Pakistani Rupees.

## **Number of GC Clause F**

### **Payment terms:**

Payment will be made to the Bidder against the procured Goods and services according to the actual invoice or running bills submitted by the Bidder against the services provided within the time given in the conditions of the contract.

## **Number of GC Clause F**

### **Identifying Defects:**

The Authority reserves the right at any time to inspect the premises of the provider to inspect the goods and monitor the goods being provided.

## **Number of GC Clause F 5 &6**

### **Following is the guidance for Dispute Resolution**

1. If any dispute of any kind whatsoever shall arise between the Authority and the Bidder in connection with or arising out of the Contract, including without prejudice to the generality of foregoing, any question regarding its existence, validity, termination and the execution of the Contract – whether during developing phase or after their completion and whether before or after the termination, abandonment or breach of the Contract – the parties shall seek to resolve any such dispute or difference by mutual diligent negotiations in good faith within 14 (fourteen) days following a notice sent by one Party to the other Party in this regard.
2. At future of negotiation the dispute shall be resolved through mediation and mediator shall be appointed with the mutual consent of the both parties.
3. At the event of failure of mediation to resolve the dispute relating to this contract such dispute shall finally be resolved through binding Arbitration by sole arbitrator in accordance with Arbitration Act 1940. The arbitrator shall be appointed by mutual consent of the both parties. The Arbitration shall take place in Islamabad, Pakistan and

proceedings will be conducted in English language.

4. The cost of the mediation and arbitration shall be shared by the parties in equal proportion however the both parties shall bear their own costs and lawyer's fees regarding their own participation in the mediation and arbitration. However, the Arbitrator may make an award of costs upon the conclusion of the arbitration making any party to the dispute liable to pay the costs of another party to the dispute.

5. Arbitration proceedings as mentioned in the above clause regarding resolution of disputes may be commenced prior to, during or after completion of the contract.

Notwithstanding any reference to the arbitration herein, the parties shall continue to perform their respective obligations under the Contract unless they otherwise agree that the Authority shall pay the Bidder any monies due to the Bidder.

**Arbitrator's fee:**

The fee shall be specified in Pak Rupees, as determined by the Arbitrator, which shall be shared equally by both parties.

**Appointing Authority for Arbitrator:**

By the Mutual Consent or in accordance with the provisions of Arbitration Act, 1940, in case the parties fail to reach a consensus on the name of sole arbitrator, any party may submit an application to the Chief Justice Islamabad High Court for appointment of sole arbitrator. The Chief Justice IHC may appoint a former judge of any High Court or Supreme Court as the sole arbitrator to resolve the dispute between the parties.

**Rules of procedure for arbitration proceedings:**

Any dispute between the Authority and a Bidder who is a national of the Islamic Republic of Pakistan arising in connection with the present Contract shall be referred to adjudication or arbitration in accordance with the laws of the Islamic Republic of Pakistan including Arbitration Act 1940, however above provision shall prevail in referring the case to the Arbitrator.

**Place of Arbitration and Award:**

The arbitration shall be conducted in English language and place of arbitration shall be at Islamabad. The award of the arbitrator shall be final and shall be binding on the parties.



## Bid Securing Declaration

## Form 9: Bid Securing Declaration

Date: *[insert date (as day, month and year)]*

Bid No.: **P44738**

To: **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).**

We, the undersigned, declare that:

We understand that, according to your conditions, Bids must be supported by a Bid Securing Declaration.

We accept that we will be blacklisted and henceforth cross debarred for participating in respective category of public procurement proceedings for a period of (not more than) six months, if fail to abide with a bid securing declaration, however without indulging in corrupt and fraudulent practices, if we are in breach of our obligation(s) under the Bid conditions, because we:

1. have withdrawn or modified our Bid during the period of Bid Validity specified in the Form of Bid;
2. Disagreement to arithmetical correction made to the Bid price; or
3. having been notified of the acceptance of our Bid by the Procuring Agency during the period of Bid Validity, (i) failure to sign the contract if required by Procuring Agency to do so or (ii) fail or refuse to furnish the Performance Security or to comply with any other condition precedent to signing the contract specified in the Bidding Documents.

We understand this Bid Securing Declaration shall expire if we are not the successful

Bidder, upon the earlier of (i) our receipt of your notification to us of the name of the successful Bidder; or (ii) twenty-eight (28) days after the expiration of our Bid.



Contract Form

## SECTION IX: CONTRACT FORMS

THIS AGREEMENT made the \_\_\_\_\_ day of \_\_\_\_\_ 20\_\_\_\_ between **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).**

(hereinafter called “the Procuring Agency”) of the one part and [name of Bidder] of [city and country of Bidder] (hereinafter called “the Bidder”) of the other part:

WHEREAS the Procuring Agency invited Bids for provision of goods, viz., **OGDCL Cyber Risk Reinsurance Coverage (P44738)** and has accepted a Bids by the Bidder for the provision of Goods in the sum of [contract price in words and figures] (hereinafter called “the Contract Price”).

### NOW THIS CONTRACT WITNESSETH AS FOLLOWS:

1. In this Contract words and expressions shall have the same meanings as are respectively assigned to them in the Conditions of Contract referred to.

2. The following documents shall be deemed to form and be read and construed as part of this Contract, In the event of any ambiguity or conflict between the Contract Documents listed below, the order of precedence shall be the order in which the Contract Documents are listed below:-

1. This form of Contract;
2. the Form of Bids and the Price Schedule submitted by the Bidder;
3. the Schedule of Requirements;
4. the Technical Specifications;
5. the Special Conditions of Contract;
6. the General Conditions of the Contract;
7. the Procuring Agency’s Letter of Acceptance; and

8. [add here: any other documents]

3. In consideration of the payments to be made by the Procuring Agency to the Bidder as hereinafter mentioned, the Bidder hereby covenants with the Procuring Agency to provide the Goods related services and to remedy defects therein in conformity in all respects with the provisions of the Contract.

4. The Procuring Agency hereby covenants to pay the Bidder in consideration of the provision of Goods and the remedying of defects therein, the Contract Price or such other sum as may become payable under the provisions of the contract at the times and in the manner prescribed by the contract.

IN WITNESS whereof the parties hereto have caused this Contract to be executed in accordance with their respective laws the day and year first above written.

Signed, sealed, delivered by \_\_\_\_\_ the \_\_\_\_\_ (for the Procuring Agency)

Witness to the signatures of the Procuring Agency:

.....

Signed, sealed, delivered by \_\_\_\_\_ the \_\_\_\_\_ (for the Procuring Agency)

Witness to the signatures of the Bidder: .....





Integrity Pact

## Integrity Pact

### **DECLARATION OF FEES, COMMISSION AND BROKERAGE ETC. PAYABLE BY THE SUPPLIERS OF GOODS, SERVICES & WORKS IN CONTRACTS WORTH RS.10.00 MILLION OR MORE**

**Contract** Number: Contract Value: Contract Title:

Dated:

[Name of Supplier] hereby declares that it has not obtained or induced the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing [Name of Supplier] represents and warrants that it has fully declared the brokerage, commission, fee etc. paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultations fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[Name of Supplier] certifies that it has made and will make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or will not take any action to circumvent the above declaration, representative or warranty.

[Name of Supplier] accepts full responsibility and strict liability for making and false declaration, not making full disclosure, misrepresenting fact or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other right and remedies available to GoP under any law, contract or other instrument, be voidable at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [Name of Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by [Name of Supplier] as aforesaid for the purpose of obtaining or inducing the procurement of any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.



## Performance Guarantee Form

## Performance Guarantee Form

To: **Pakistan Reinsurance Company Limited (PAKRE) (Ministry of Commerce), Procurement Specialist PRC Tower, 32-A, Lalazar Drive, M.T. Khan Road., Civil Line Sub-Division, Karachi South (District), Karachi (Division), Sindh (Province).**

WHEREAS *[name of Bidder]* (hereinafter called “the Bidder”) has undertaken, in pursuance of Contract No. *[reference number of the contract]* dated *[insert date]* for provision of Goods (hereinafter called “the Contract”).

AND WHEREAS it has been stipulated by you in the said Contract that the Bidder shall furnish you with a Bank Guarantee by a reputable bank for the sum specified therein as security for compliance with the Bidder’s performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Bidders guarantee:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Bidder, up to a total of *[amount of the guarantee in words and figures]*, and we undertake to pay you, upon your first written demand declaring the Bidder to be in default under the Contract and without cavil or argument, any sum or sums within the limits of *[amount of guarantee]* as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the: *[insert date]*

Signature and seal of the Guarantors

---

*[name of bank or financial institution]*

---

*[address]*

---

*[date]*



Annexure

## Terms & Conditions

These terms & conditions must be signed and stamped by the bidder

Technical Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Terms & Conditions** (page number: 65)

## Policy Wording

document must be signed and stamped by the bidder.

Technical Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Policy Wording** (page number: 70)

## Proposal Form

must be signed and stamped by the bidder.

Technical Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Proposal Form** (page number: 122)

## Technical Evaluation Criteria

must mention compliance yes/no & signed stamped by the bidder.

Technical Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Technical Evaluation Criteria** (page number: 150)

## Financial Matrix

must be signed stamped by the bidder.

Financial Submission (Vendor)

Document Required

See Form Under Additional Forms and Documents: **Financial Matrix** (page number: 151)





## Procurement Forms







## Additional Forms and Documents



# Pakistan Reinsurance Company Limited

(Under the administrative control of Ministry of Commerce, Government of Pakistan)

PRC Towers, 32-A, Lalazar Drive, M.T. Khan Road, Karachi, Pakistan

Ph: 021-99202908- 14 Fax: (92-21) 99202920-21 & 22

[prcl@pakre.org.pk](mailto:prcl@pakre.org.pk), Website: [www.pakre.org.pk](http://www.pakre.org.pk)

## **TERMS AND CONDITIONS FOR TENDER NO. 138(PRCL-RETRO-OGDCL-CYBER REINSURANCE)/2026**

1. Bidder should be an international (re)insurance broker having an annual premium placement volume of at least USD 500 million, evidence of which must be submitted with bids. The international broker should submit the bid directly. The local affiliate, must have a valid SECP license, NTN, Sales Tax (if services are taxable), and on active taxpayers' list of FBR. PRCL may any time ask for a foreign and local broker's written agreement or MOU etc. Nevertheless, the (re)insurance premium will only be paid/transferred into a foreign broker's account, whose signed and stamped slips are submitted with bids and similarly, refund/adjustment premiums, Claims proceed, if any, should be transferred by the foreign broker directly into PRCL's account. Foreign broker as well as local affiliate both are required to submit copies of their respective valid professional indemnity policies meeting regulatory requirements of their respective countries of registration.
2. The participating broker shall be required to submit the prescribed KYC/UBO forms/documents filled by the Leader/ Leaders (if allowed) as part of their technical bid and Follow Markets (within one (1) month from the date of award of contract/placement order.
3. One Bidder (international broker) can submit only one bid; more than one bid(s) received from one broker will be liable to rejection.
4. Bidder shall not be blacklisted by any Government Agency/Institution of Pakistan. The bidder shall affirm this condition in their technical submission. However, temporary blacklist firm/bidder can submit bid if the blacklisting period has ended before the bid submission date.
5. Bidder who wishes to participate in this tender shall also intimate the name, contact number, and e-mail address of its authorized representative. Only the authorized representative shall be allowed to communicate with PRCL, seek clarification, participate in pre-bid conference/bid opening, etc. Further please note that any email from local affiliated brokers, if sent without keeping in loop international broker, the same will not be entertained by PRCL. Hence, international brokers must be kept in the loop in all emails/correspondences with PRCL.
6. Bidder must submit a signed/ stamped compliance matrix that must be on foreign broker's letter-head with their Technical bid and premium calculations with their financial bid as per the format provided with this letter.
7. Bid should be a FIRM QUOTE (not an indication or subject to 'Best Terms'). Price change/variation after opening of bids may lead to disqualification of the bidder/rejection of the bid.



# Pakistan Reinsurance Company Limited

(Under the administrative control of Ministry of Commerce, Government of Pakistan)

PRC Towers, 32-A, Lalazar Drive, M.T. Khan Road, Karachi, Pakistan

Ph: 021-99202908- 14 Fax: (92-21) 99202920-21 & 22

[prcl@pakre.org.pk](mailto:prcl@pakre.org.pk), Website: [www.pakre.org.pk](http://www.pakre.org.pk)

8. Leader's written confirmation must be submitted by the broker to support any clarification/correction in their bid/policy wording that may be provided by them in response to PRCL's request.
9. Bid should be without any expressed or implied subjectivities/conditions/additional exclusions and warranties otherwise it may lead to disqualification.
10. All non-conditional discounts (e.g., Client and special Discounts etc) must be separately mentioned in the bid. PRCL will include these discounts in financial evaluation.
11. All conditional discounts and bonuses (e.g., No claim bonus, prompt payment discount, and continuity discount) must separately be mentioned in the bid. Being conditional such discounts/bonuses whether upfront or otherwise, will not be included in the financial evaluation/comparison. Only in case of a tie such conditional discounts/bonuses will be included in comparison.
12. Bidder shall ensure that the lead reinsurer, whose quote is being submitted, shall later be reflected in the placement sheet with the required lead share. The cover note/policy wording must also be signed by the same leader with the share quoted in bid.
13. Bidder must provide risk-wise break up along with the premium for each section as well as the aggregate premium in their financial bid. A computation sheet summarizing the gross premium/price to net premium/price working shall also be submitted
14. The bidder whose submission (i) is compliant with evaluation criteria and other conditions of the bidding documents and client requirements and (ii) having lowest evaluated bid shall be declared as the successful bidder.
15. Successful bidder shall complete placements at the earliest but not later than 15 days from the date of issuance of the placement order.
16. The size of reinsurance order to the winning broker of this tender shall be advised by the PRCL at the time of order placement that may vary from the reinsurance order placed with the incumbent broker for the expiring period.
17. If requested by the client or circumstances so warrant during the reinsurance period, the incumbent broker may be asked for amendment(s) in the scope of cover &/or additions / deletions in the items covered &/or increase / decrease in the sum(s) insured / limit(s) of liability / deductible(s) etc. The terms and conditions of these endorsements will be mutually agreed upon by all the parties involved.



# Pakistan Reinsurance Company Limited

(Under the administrative control of Ministry of Commerce, Government of Pakistan)

PRC Towers, 32-A, Lalazar Drive, M.T. Khan Road, Karachi, Pakistan

Ph: 021-99202908- 14 Fax: (92-21) 99202920-21 & 22

[prcl@pakre.org.pk](mailto:prcl@pakre.org.pk), Website: [www.pakre.org.pk](http://www.pakre.org.pk)

18. If requested by the client or circumstances so warrant the incumbent broker may be asked to arrange extension(s) in the period of reinsurance cover. The time span of such extension(s) may be for one or more full policy periods or less than a full policy period. The terms and conditions of these extensions will be mutually agreed upon by all the parties involved. Further, in case a discount is offered by the incumbent broker/reinsurer in lieu of an LTA (Long Term Agreement) or Extension of the reinsurance covers for multiple years, the same may be accepted by PRCL on insured's approval thereto.
19. In case of appointed broker's poor services especially with regards to the claim(s) recoveries under the cover in question whether slow &/or no response to the client's/PRCL's emails/correspondence &/or delay in collection of claims proceeds from the relevant reinsurers &/or delay in transferring claims proceeds so collected to PRCL, the contract awarded to the broker as a result of this tender may be discontinued before completion of its full period and the brokers (foreign and their local affiliates) may also be debarred from participating subsequent PRCL tenders till their issues are resolved to the full satisfaction of PRCL.
20. Name of the leader along with the country of origin and current rating must be advised by the bidder at the time of submitting the bid. Share of the lead reinsurer must be at least 15% and not more than 25% and must hold at minimum "A" rating per S&P/ AM Best/ Moodys/ Fitch that should be clearly confirmed by the bidder in their technical Bid. Separate leaders are allowed on each layer but the lead share in each individual layer must be not less than 15% and not more than 25% of that respective layer.
21. The remaining risk must also be placed with minimum "A- " securities or above as per the rating signed by S&P/ AM Best/ Moody's/Fitch. Managing General Agencies and Underwriting Agencies who write the risk on behalf of minimum A- rated securities (signed by S&P/ AM Best/ Moody's/Fitch) are allowed to be used as follow/support market up to 20% of 100%, but in no case, any Managing General agency and underwriting agency (irrespective of its principal or owner) is allowed to be used as leader. Further, Takaful/Re-takaful/Operator/Company are not allowed even as a follower.
22. Quoted rate must be valid at least for 45 days from the date of bid opening and the bidder must affirm this in their technical submissions.
23. Premium Payment Warranty (PPW) should be of 90 days from the inception of the policy period.
24. The quote submitted by the bidder should include 10% reinsurance commission that must be paid to NICL/PRCL by the successful bidder. Further, the bidder should provide stepwise computation to



# Pakistan Reinsurance Company Limited

(Under the administrative control of Ministry of Commerce, Government of Pakistan)

PRC Towers, 32-A, Lalazar Drive, M.T. Khan Road, Karachi, Pakistan

Ph: 021-99202908- 14 Fax: (92-21) 99202920-21 & 22

[prcl@pakre.org.pk](mailto:prcl@pakre.org.pk), Website: [www.pakre.org.pk](http://www.pakre.org.pk)

- 
- arrive at the 100% Net to Broker Amount from the 100% markets gross premium i.e. deduction(s) of discounts and reinsurance commission payable to NICL/PRCL etc.
25. No additional premium or differential premium other than the leader's quoted rate/ premium shall be allowed. Therefore, the Broker has to complete the entire reinsurance order placement within the leader's quoted rate.
  26. PRCL has the right to cancel the contract at any time if it is found that the bidder was non-compliant with the terms and conditions regarding placement mentioned in the bidding documents. However, in case of non-compliance, 15 days' time to comply shall be given. In case of failure, PRCL may take action as deemed appropriate.
  27. In the event of a dispute arising between PRCL and the successful bidder/ reinsurers, out of or in connection with the contract, such dispute shall be amicably settled through negotiations. If the dispute remains unsettled for 30 days, the parties may resort to Arbitration. The Arbitration shall be subject to the Arbitration Act of 1940 (Pakistan Law). The law and jurisdiction for arbitration/litigation must be that of the Islamic Republic of Pakistan.
  28. Any query relating to the risk should be shared with PRCL 05 days prior to the bid opening date.
  29. Direct Communication by the broker with the client/insured/NICL without keeping in loop the procuring agency i.e. PRCL is against the rules hence not allowed at any stage of the tender and even after placement of reinsurance order as well as during/after commencement of reinsurance cover. If is done, it may lead to disqualification of that broker. Requests for road shows and risk surveys should also be addressed to PRCL only without involving NICL and insured, as PRCL will take-up such requests of broker with them and revert.
  30. If any participant/broker use unethical/threatening wording/language it may lead to their disqualification.
  31. Internal procurement committee(s) of PRCL shall evaluate all bids.
  32. PRCL has the right to extend the date of opening of the bid or to cancel the bidding process if required, and issue addendums, corrigendum, and modifications to any or all conditions of bidding documents prior to the opening of bids.
  33. PRCL does not bind itself to accept the lowest or any quote (if technically non-compliant) and as per above stated conditions and reserves it's right to accept and/ or reject any or all offers/bids without assigning any reasons.



## Pakistan Reinsurance Company Limited

(Under the administrative control of Ministry of Commerce, Government of Pakistan)

PRC Towers, 32-A, Lalazar Drive, M.T. Khan Road, Karachi, Pakistan

Ph: 021-99202908- 14 Fax: (92-21) 99202920-21 & 22

[prcl@pakre.org.pk](mailto:prcl@pakre.org.pk), Website: [www.pakre.org.pk](http://www.pakre.org.pk)

---

34. Complaints/grievances (if any) will be entertained as per PPRA guidelines.



**RISK DETAILS**

**UNIQUE MARKET REFERENCE:** TBC

**TYPE:** Network Security and Privacy Liability (Cyber Risks) Reinsurance

**ORIGINAL INSURED:** Oil & Gas Development Company Limited

**ORIGINAL INSURED'S ADDRESS:** Plot No 3,OGDCL Building, Jinnah Avenue F6/1, Blue Area, Islamabad, 44000

**POLICY PERIOD:** 12 Month (date to be advised)  
Both days inclusive Local Standard Time at the Insured's address detailed above

**INTEREST:** As per policy

**LIMIT OF LIABILITY (100%):** USD 10,000,000 each and every claim and in the aggregate including costs and expenses  
**The overall Aggregate limit of indemnity for all Insuring Clauses is USD 10,000,000**

**SUBLIMITS OF LIABILITY**

|                       |                             |  |
|-----------------------|-----------------------------|--|
| First Response:       | Period                      | 72 Hours   |
|                       | Emergency Number:           | TBC  |
|                       | IT Specialist               | TBC  |
|                       |                             | 100% of Limit of Liability in the annual aggregate |
| Network Interruption: | Security Failure Cover:     | 100% of Limit of Liability in the annual aggregate |
|                       | System Failure Cover:       | 100% of Limit of Liability in the annual aggregate |
|                       | OSP Security Failure Cover: | 100% of Limit of Liability in the annual aggregate |

|                               |  |
|-------------------------------|--|
| OSP System Failure Cover:     | 100% of Limit of Liability in the annual aggregate     |
| Voluntary Shutdown Cover:     | 100% of Limit of Liability in the annual aggregate     |
| Loss Preparation Costs Cover: | USD 100,000 Limit of Liability in the annual aggregate |
| Reputational Harm:            | 100% of Limit of Liability in the annual aggregate     |

Cyber Extortion: 100% of Limit of Liability in the annual aggregate

Event Management: 100% of Limit of Liability in the annual aggregate

Security and Privacy Liability: 100% of Limit of Liability in the annual aggregate

Loss Prevention Services: Included

Criminal Reward Fund: USD 50,000 of Limit of Liability in the annual aggregate

Digital Media Content Liability: 100% of Limit of Liability in the annual aggregate

Bricking Extension Endorsement: 100% of Limit of Liability in the annual aggregate

**DEDUCTIBLE:**

General Policy Deductible:  
USD 250,000 each and every claim

Network Interruption Loss Waiting Hours:  
12 Hours

Loss Preparation Costs:  
No Retention

First Response:  
No Retention

Criminal Reward Fund:

No Retention

Reputational Harm:

14 Days

**TERRITORIAL LIMITS:** Worldwide

**ORIGINAL  
CONDITIONS:**

It is hereby noted and agreed that the Reinsurance Policy hereunder shall follow all the terms, clauses, exceptions, warranties and conditions of original policy wording as attached, and to follow its settlements subject however to the terms and conditions of this agreement:

1. Claims Control and Settlement Clause
2. Premium Payment Clause LSW 3001
3. Continuity Date/Prior and Pending Claims and Circumstances
4. Network Interruption Coverage Section
5. Cyber Extortion Coverage Section
6. Event Management Coverage Section
7. Security and Privacy Liability Coverage Section
8. Criminal Reward Fund
9. Digital Media Content Liability
10. Territory Restriction Endorsement
11. War and Terrorism Exclusion Amended Endorsement
12. Bricking Extension Endorsement
13. Reputational Harm Coverage Section

**LAW AND  
JURISDICTION:**

The (re)insurance shall be governed by the construed in accordance with the law of the Pakistani courts, Pakistan and each party agrees to submit to the exclusive jurisdiction of the Courts of Pakistan.

**PREMIUM:**

**PREMIUM PAYMENT  
TERMS:**

90 days – 15 days prior notice - Premium Payment Condition LSW3001, as attached.

## **PREMIUM PAYMENT CLAUSE**

Notwithstanding any provision to the contrary within this contract or any endorsement hereto, in respect of non payment of premium only the following clause will apply.

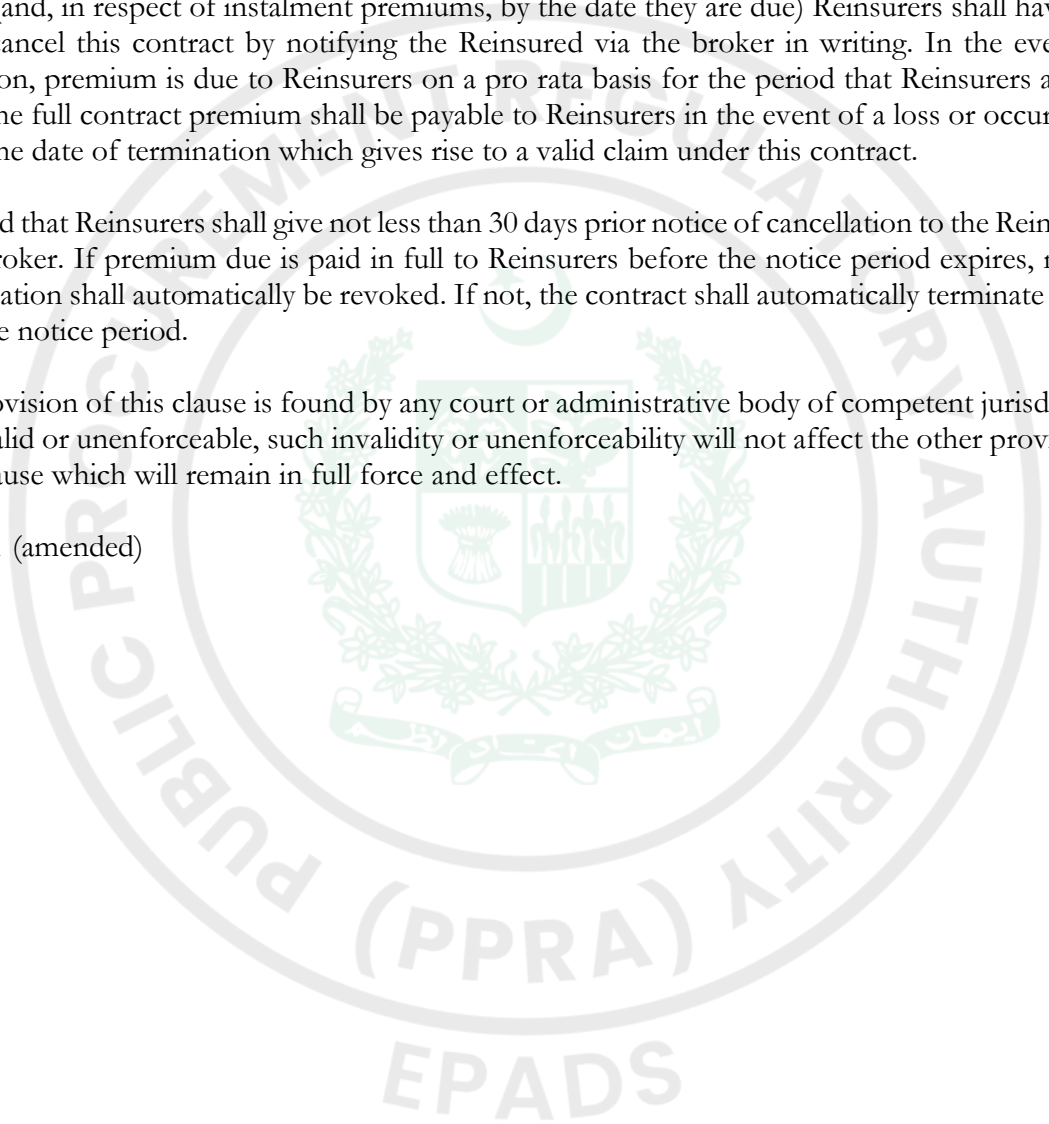
The Reinsured undertakes that premium will be paid in two equal instalments to Reinsurers within 90 (1<sup>st</sup> instalment) and 180 (2<sup>nd</sup> instalment) days of inception of this contract (or in respect of instalment premiums, when due).

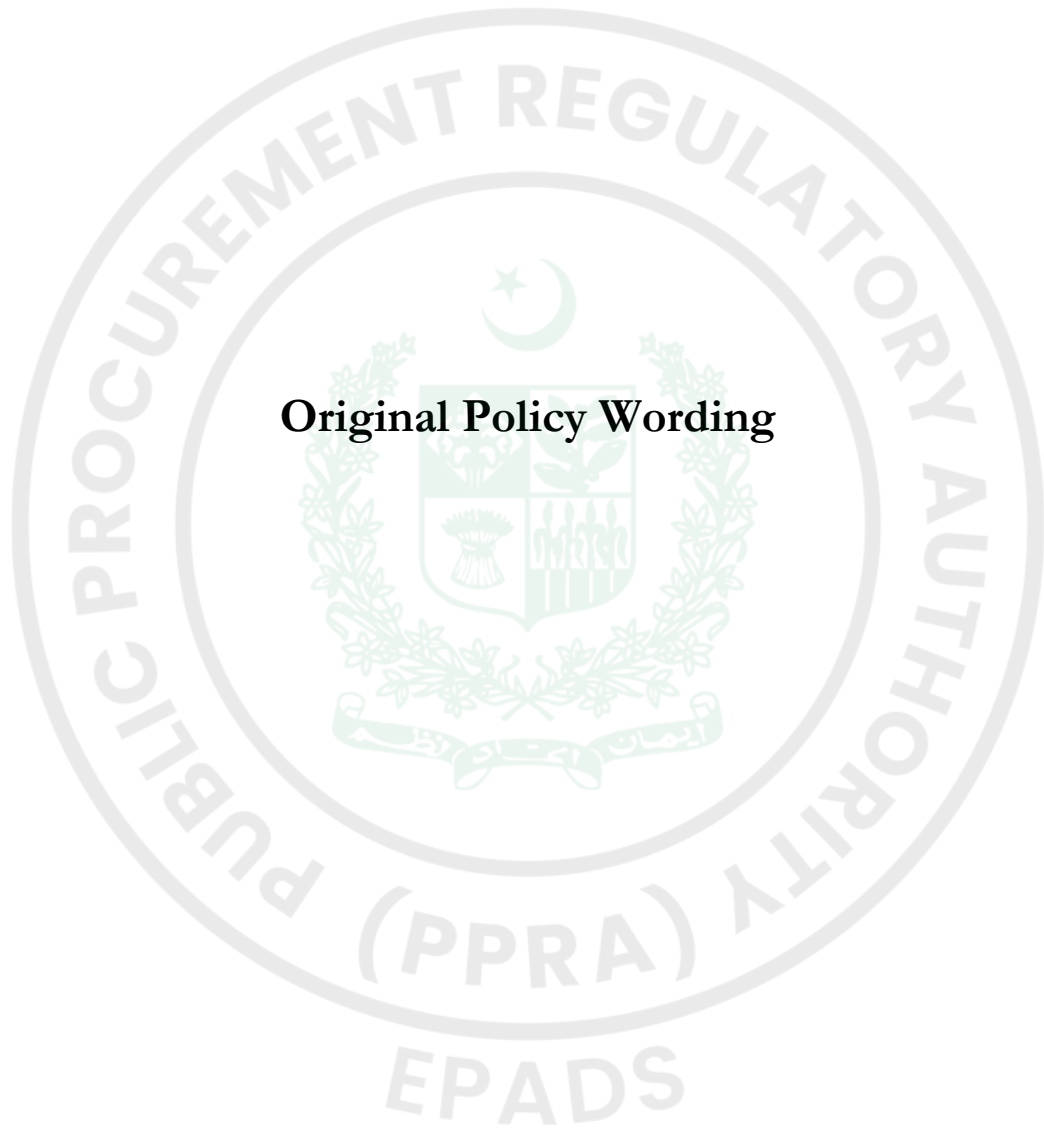
If the premium due under this contract has not been so paid to Reinsurers by the due dates of this contract (and, in respect of instalment premiums, by the date they are due) Reinsurers shall have the right to cancel this contract by notifying the Reinsured via the broker in writing. In the event of cancellation, premium is due to Reinsurers on a pro rata basis for the period that Reinsurers are on risk but the full contract premium shall be payable to Reinsurers in the event of a loss or occurrence prior to the date of termination which gives rise to a valid claim under this contract.

It is agreed that Reinsurers shall give not less than 30 days prior notice of cancellation to the Reinsured via the broker. If premium due is paid in full to Reinsurers before the notice period expires, notice of cancellation shall automatically be revoked. If not, the contract shall automatically terminate at the end of the notice period.

If any provision of this clause is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, such invalidity or unenforceability will not affect the other provisions of this clause which will remain in full force and effect.

LSW3001 (amended)





**Original Policy Wording**

# Network Security and Privacy Insurance

## General Terms and Conditions

In consideration of the payment of **Premium** or agreement to pay the **Premium**, the **Policyholder** and the **Insurer** agree as follows:

### 1. Application of General Terms and Conditions

---

These **General Terms and Conditions** shall apply to all **Coverage Sections**, unless a **Coverage Section** states specifically that all or part of these **General Terms and Conditions** shall not apply to that **Coverage Section**. The terms and conditions set forth in each **Coverage Section** shall only apply to that particular **Coverage Section**. The definitions shall have the meaning given to them either in Section 10. (Definitions) of these **General Terms and Conditions** or in the **Coverage Section** they are used in.

### 2. Cover

---

The **Insurer** will provide insurance cover as set out in those **Coverage Sections** which are **Purchased**.

### 3. Limits of Liability

---

The total amount payable by the **Insurer** under this policy for the **Policy Period** for all **Loss** in the aggregate arising from all **Insured Events** covered by this policy shall not exceed the **Policy Aggregate Limit of Liability**.

In respect of each **Coverage Section**, the total amount payable by the **Insurer** under this policy for the **Policy Period** for all **Loss** in the aggregate arising from all **Insured Events** covered by that **Coverage Section** shall not exceed that **Coverage Section's Coverage Section Limit of Liability**. Each **Coverage Section Limit of Liability** is part of and not in addition to the **Policy Aggregate Limit of Liability**. Payments of **Loss** under any **Coverage Section** shall erode the **Policy Aggregate Limit of Liability**.

The total amount payable by the **Insurer** for **Loss** in respect of which a sub-limit is specified in the schedule or any other provision of this policy shall not exceed that sub-limit. Sub-limits are part of and not in addition to the **Policy Aggregate Limit of Liability** and the **Coverage Section Limit of Liability** of the **Coverage Section** which covers the **Loss**. Each such sub-limit is, unless specifically stated otherwise, for the **Policy Period** for all **Loss** in the aggregate arising from all **Insured Events** covered by this policy.

Amounts specified for the **Policy Aggregate Limit of Liability**, **Coverage Section Limits of Liability**, sub-limits and other limits are limits for all **Insureds** together, not limits per **Insured**.

### 4. Retentions

---

With respect to each **Single Insured Event**, the **Insurer** shall only pay that part of **Loss** which exceeds the **Retention**. The **Insurer** may, in its sole and absolute discretion, advance **Loss** within the **Retention**, and, in that event, such amounts shall be reimbursed to the **Insurer** by the **Policyholder** forthwith.

The **Retention** is to be borne by the **Insureds** and shall remain uninsured. In the event that a **Single Insured Event** triggers more than one **Retention**, then, as to such **Single Insured Event**, the highest of those **Retentions** shall be in effect with regard to the **Loss**.

The **Retentions** for each **Coverage Section** are set out in the schedule. The application of a **Retention** to **Loss** under one **Coverage Section** shall not reduce the **Retention** under any other **Coverage Section**.

### 5. Subrogation

---

Where any amount is paid under this policy in respect of an **Insured Event**, the **Insurer** shall be subrogated to all rights of recovery of each **Insured** (whether or not the **Insured** has been fully compensated for its actual loss). The **Insurer** shall be entitled to pursue and enforce such rights in the name of the **Insured** and the **Insured** shall provide the **Insurer** with

all reasonable assistance and co-operation in this regard including the execution of any necessary documents. No **Insured** shall do anything to prejudice the **Insurer's** rights of recovery.

A **Company** may waive an **Insured's** rights to recovery against others if such **Company** does so in writing and before the **Insured Event** occurred.

## 6. Recoveries

---

In the event the **Insurer** recovers amounts it pays under this policy, the limits and sub-limits out of which those amounts are paid shall be replenished to the extent of the recovery less any costs of recovery.

Amounts recovered in excess of the **Insurer's** total payment under this policy (less any costs of recovery) shall be returned to the relevant **Insured**.

The **Insurer** assumes no duty to seek a recovery of any amounts paid under this policy.

## 7. Optional Discovery Period

---

If this policy is not renewed or replaced, the **Policyholder** shall, solely with respect to the **Specified Professions Professional Liability, Media Professional Liability and Technology Professional Liability Coverage Sections**, be entitled to purchase one of the following **Discovery Periods**:

- (i) a period of 1 year for an additional premium of 100% of the **Full Annual Premium**;
- (ii) a period of 2 years for an additional premium of 175% of the **Full Annual Premium**;
- (iii) a period of 3 years for an additional premium of 200% of the **Full Annual Premium**.

To make the purchase, the **Policyholder** must give written notice to the **Insurer** and pay the additional premium no later than 30 days after the expiry of the **Policy Period**. There shall be no entitlement to purchase a **Discovery Period** after those 30 days.

A **Discovery Period** purchased pursuant to this Section 7 (Optional Discovery Period):

- (a) shall incept at the end of the **Policy Period**;
- (b) shall not apply to any **Insured Event** covered under any renewal or replacement of this policy (or any policy providing similar cover); and
- (c) cannot be cancelled (and the additional premium charged for it shall be fully earned at its inception).

## 8. Claims

---

### 8.1. Notice and Reporting

It is a condition precedent to the **Insurer's** liability under this policy for **Loss** arising from an **Insured Event**:

- (i) that the **Insurer** is given written notice of that **Insured Event** as soon as practicable after a **Company's Responsible Officer** first becomes aware of it; and
- (ii) that the **Insurer** is given written notice of any circumstances that a **Company's Responsible Officer** may become aware of and which may reasonably be expected to give rise to that **Insured Event** as soon as practicable following that awareness,

but in all events, no later than:

- (a) 60 days after the end of the **Policy Period**; or
- (b) expiry of any applicable **Discovery Period**.

A notice of circumstances which may reasonably be expected to give rise to an **Insured Event** must include, to the extent known after reasonable inquiry, the reasons for anticipating the **Insured Event** and particulars as to dates, acts and the potential **Insureds** and claimants concerned.

Where the First Response Cover is **Purchased** and a **Company** has notified the **Insurer** of an **Insured Event** by calling the Emergency Number specified in the schedule, then, provided the **Insurer** has acknowledged the call, the **Company** does not need to also provide written notice to the **Insurer** as set out in this Section 8.1 (Notice and Reporting).

## 8.2. Related Claims, Insured Events or Circumstances

If a **Claim**, other **Insured Event** or circumstance is notified in writing to the **Insurer** as required by Section 8.1 (Notice and Reporting) of these **General Terms and Conditions**, then all subsequent **Claims**, other **Insured Events** and circumstances that constitute a **Single Insured Event** with that notified **Claim**, other **Insured Event** or circumstance shall be:

- (i) deemed to have been first made (in the case of **Claims**), to have first occurred (in the case of other **Insured Events**) and to have been first notified (in the case of circumstances) at the time when that notified **Claim**, other **Insured Event** or circumstance (respectively) was first made, first occurred or was first notified; and
- (ii) deemed to be notified to the **Insurer** at the time that required or permitted notice was given.

For the purposes of this Section 8.2 (Related Claims, Insured Events or Circumstances), a circumstance which may reasonably be expected to give rise to an **Insured Event** and which is notified in writing to the **Insurer** as required by Section 8.1 (Notice and Reporting) of these **General Terms and Conditions** shall be deemed to be an **Insured Event**.

## 8.3. Defence and Settlement

The **Insurer** has the right but no obligation to defend any **Claim** or **Regulatory Investigation**. Each **Insured** shall have the obligation to defend and contest a **Claim** or **Regulatory Investigation** made against them unless the **Insurer**, in its sole and absolute discretion, elects in writing to take over and conduct the defence and settlement of the **Claim** or **Regulatory Investigation**. If the **Insurer** does not so elect, it shall be entitled, but not required, to participate fully in that defence and the negotiation of any settlement that involves or appears reasonably likely to involve the **Insurer** making a payment under this policy.

If legal representation is necessary in relation to any **Insured Event**, the **Insurer** shall select a law firm from its legal panel to provide such legal representation. Should an **Insured** wish to appoint a different law firm, that **Insured** shall make the request in writing to the **Insurer** prior to retaining that law firm. Such request shall include the identity of the proposed fee earners, the proposed hourly rates for each fee earner, a summary of the firm's and those fee earners' experience in handling similar matters and a budget for the **Insured Event**. The **Insurer** shall not be obliged to agree to the request.

The **Insurer** has the right at any time after notification of an **Insured Event** to make a payment to the **Insured** of the unpaid balance of the **Coverage Section Limit of Liability** (or, if a sub-limit is applicable to that **Insured Event**, the unpaid balance of that sub-limit), and upon making such payment, all obligations of the **Insurer** under this policy for that **Insured Event**, including, if any, those relating to defence of such **Insured Event**, shall cease.

### 1.1. Insurer's Consent

No **Insured** shall admit or assume any liability, enter into any settlement agreement, consent to any judgment, incur any **Defence Costs** or incur any other amounts where consent is required under this policy without the prior written consent of the **Insurer** (which shall not be unreasonably withheld or delayed, provided that the **Insurer** shall be entitled to exercise all of its rights under the policy). Only liabilities, settlements, judgments and **Defence Costs** (and other amounts where consent is required under this policy) consented to by the **Insurer**, and judgments resulting from **Claims** defended in accordance with this policy or other **Insured Events** handled in accordance with this policy, shall be recoverable as **Loss** under this policy.

Notifying a **Regulator** of an actual or potential **Breach of Confidential Information** or breach of **Data Protection Legislation** will not be regarded as an admission of liability for the purposes of this Section 1.1 (Insurer's Consent).

### 1.2. Insured's Consent

The **Insurer** may make any settlement of any **Insured Event** it deems expedient with respect to any **Insured**, subject to such **Insured's** written consent (which shall not be unreasonably withheld or delayed). If any **Insured** withholds or delays consent to such settlement, the **Insurer's** liability for all **Loss** arising from such **Insured Event** shall not exceed the amount for which the **Insurer** could have settled such **Insured Event**, plus **Defence Costs** (and other costs covered by this policy in relation to that **Insured Event**) incurred as of the date such settlement was proposed in writing by the **Insurer**, less coinsurance (if any) and the applicable **Retention**.

### 1.3. Cooperation

Each **Insured** will at their own cost:

- (i) provide all reasonable assistance to the **Insurer** and co-operate in the investigation, defence, settlement or appeal of any **Insured Event** 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; and
- (iii) 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.

### 1.1. Other Insurance

The **Network Interruption, Event Management** and **Cyber Extortion Coverage Sections** are written on a primary basis.

Each other **Coverage Section** shall always apply excess over any other valid and collectable insurance unless such other insurance is expressly written to be excess over the **Policy Aggregate Limit of Liability** or that **Coverage Section's Coverage Section Limit of Liability**.

### 1.2. Allocation

In the event that any **Insured Event** involves both covered matters and matters not covered under this policy or involves persons covered and persons not covered under this policy, a fair and proper allocation of any costs of defence, damages, judgments or settlements or other costs and expenses shall be made between each **Insured** and the **Insurer** taking into account the relative legal and financial exposures attributable to covered matters and matters not covered under this policy.

## 2. General Provisions

---

### 2.1. Cancellation by Policyholder

This policy may be cancelled by the **Policyholder** providing written notice to the **Insurer**. If no **Claim** has been made or other actual or alleged **Insured Event** has occurred and no circumstance has been notified prior to such cancellation, the **Insurer** shall retain the pro-rata proportion of **Premium** due for time on risk. Otherwise, the **Premium** shall not be returned and shall be deemed fully earned at the inception date specified in the schedule.

### 2.2. Cancellation by Insurer

This policy may not be cancelled by the **Insurer** except for non-payment of the **Premium** by the **Policyholder** or in accordance with clause 8.10 (Fraudulent Claims) of these **General Terms and Conditions**.

### 2.3. Insured's Insolvency

Insolvency, bankruptcy, winding up of any kind, administration, administrative receivership, voluntary arrangement or any other insolvency procedure of an **Insured** shall not relieve the **Insurer** of any of its obligations under this policy.

### 2.4. Authority of Policyholder

Except as provided in Section 8.1 (Notice and Reporting) of these **General Terms and Conditions**, the **Policyholder** shall act on behalf of all **Insureds** with respect to all matters relevant to this policy except if and when the **Policyholder** is in

bankruptcy, winding up of any kind, administration, administrative receivership, voluntary arrangement or any other insolvency procedure, in which case each **Insured** shall act on their own behalf.

#### **8.4. Assignment**

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

#### **8.5. Governing Law**

This policy and any disputes or claims arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the laws of England and Wales.

#### **8.6. Contracts (Rights of Third Parties) Act 1999**

No person other than an **Insured** shall have directly enforceable rights under this policy, whether pursuant to the Contracts (Rights of Third Parties) Act 1999 or otherwise.

#### **8.7. Interpretation**

The descriptions in the headings and titles of this policy are solely for reference and convenience and do not lend any meaning to this policy. Words and expressions in the singular shall include the plural and vice versa. All references to specific legislation include amendments to and re-enactments of such legislation and similar legislation in any jurisdiction in which a **Claim** is made or an **Insured Event** occurs. References to positions, offices or titles shall include their equivalents in any jurisdiction in which **Claim** is made or an **Insured Event** occurs. Words in **bold** typeface have special meaning and are defined in these **General Terms and Conditions** or in the applicable **Coverage Section**. References in this policy to the schedule or a Section mean the schedule to or a Section of this policy unless otherwise stated. Wherever the word "person" or "persons" appears in this policy, it means legal or natural person or persons unless otherwise specified.

#### **8.8. Dispute Resolution**

Except as otherwise specifically provided in this policy, any dispute arising out of or in connection with this policy or its subject matter or formation (including non-contractual disputes or claims) which cannot be resolved by agreement within 60 days, may be referred to binding arbitration by either party, upon giving 7 days' notice to the other, in the London Court of International Arbitration (LCIA), whose rules shall be deemed incorporated by reference to this clause, and the cost shall be borne equally between the **Insured** and **Insurer**. The **Insured** and the **Insurer** shall each name one arbitrator and the third shall be appointed by the LCIA. The language to be used in the arbitration proceedings shall be English. The arbitration shall be conducted by a panel of 3 arbitrators having knowledge of the legal and insurance issues relevant to the matters in dispute. The decision of the arbitrators shall be final and binding and provided to both parties, and the arbitrators shall not be asked, and shall not award attorney's fees or other costs.

#### **8.9. Duty of Fair Presentation**

##### **A. Fair Presentation**

Prior to the inception date specified in the schedule, and a variation of this policy, the **Companies** must make a fair presentation of the risk to be insured under this policy.

A fair presentation of the risk is one:

- (i) which discloses every material circumstance that the Insurance Representatives know or ought to know; or
- (ii) failing that, which gives the **Insurer** sufficient information to put a prudent **Insurer** on notice that it needs to make further enquiries for the purpose of revealing those material circumstances.

For the purposes of this clause the Insurance Representatives ought to know what should reasonably have been revealed by a reasonable search of information available to the **Companies**, including information held by the **Companies'** agents or by those for whom cover is provided by this policy; and an Insurance Representatives is

deemed to know any circumstance which he suspected, and would have known but for deliberately refraining from confirming or enquiring about it;

- (a) which makes that disclosure in a manner which would be reasonably clear and accessible to a prudent **Insurer**; and
- (b) in which every material representation:
  - (A) as to a matter of fact, is substantially correct;
  - (B) as to a matter of expectation or belief, is made in good faith.

For the purposes of this clause the "Insurance Representatives" consist of those who participate on behalf of the **Companies** in the process of procuring the **Insureds'** insurance together with the individuals who play significant roles in the making of decisions about how the **Company's** activities are to be managed or supervised.

## B. Remedies

If the above clause 8.9. A (Fair Presentation) is breached, and, but for the breach, the **Insurer**

- (i) would not have entered into the policy; or
- (ii) would have done so only on different terms,

The **Insurer** will have remedies as against the **Companies** as follows:

- (a) The **Insurer** may avoid this policy and refuse all claims if:
  - (A) the breach is deliberate or reckless, in which event the **Insurer** may retain the premium paid; or
  - (B) but for the breach the **Insurer's** underwriter would not have entered into the policy on any terms, in which event the **Insurer** shall return the premium.
- (b) In all other cases:
  - 1 where the **Insurer's** underwriter would have charged more premium, any amounts payable by the **Insurer** will be scaled down to the ratio that the premium actually charged (the "**Actual Premium**") bears to the premium that he would have charged to assume that risk (the "**Reference Premium**"); and in addition
  - 2 where the **Insurer's** underwriter would have written the risk on different terms (other than in relation to premium) the policy is to be treated as if it had been entered into on those terms.

## 8.10. Fraudulent Claims

If any **Insured** shall make a fraudulent claim under this policy, the **Insurer**:

- (i) is not liable to pay any part of the claim;
- (ii) may recover from that **Insured** any sums already paid to or on behalf of that **Insured** in respect of the claim; and
- (iii) may, by notice to that **Insured**, treat this policy as having been terminated with effect from the date of the fraudulent act, in which case the **Insurer** is not liable for any relevant event occurring after that date and is entitled to receive and retain the full **Premium**.

## 9. Definitions

Terms appearing in **bold** in these **General Terms and Conditions** and not defined in this Section 10. (Definitions) shall have the meaning ascribed to them in the applicable **Coverage Section** for the purposes of coverage provided under that particular **Coverage Section**.

Certain terms may have different meanings dependent on the applicable **Coverage Section**. Where a term is defined in more than one **Coverage Section** it shall have the meaning ascribed to it in the **Coverage Section** in which it appears, but that meaning shall apply solely for purposes of coverage provided under that particular **Coverage Section**.

The following terms are applicable to all **Coverage Sections** and shall have the meanings set out below:

### **Company**

The **Policyholder** or any **Subsidiary**.

### **Continuity Date**

With respect to a **Coverage Section** or a specific Cover within a **Coverage Section**, the date specified in the schedule as its Continuity Date.

### **Coverage Section**

A coverage section listed in the schedule. The **Insurer** will provide only the insurance cover set out in those coverage sections which are **Purchased**.

### **Coverage Section Limit of Liability**

With respect to a **Coverage Section**, the amount specified in the schedule as its Coverage Section Limit of Liability.

### **Data**

Any electronically stored, digital, or digitised information or media. For the purposes of this policy, **Data** is not tangible property.

### **Discovery Period**

a period immediately following the expiry of the **Policy Period** during which written notice may be given to the **Insurer** of a **Claim** first made during such period or the **Policy Period** for a **Wrongful Act** prior to the expiry of the **Policy Period**.

A **Claim** first made during an applicable **Discovery Period** and notified to the **Insurer** in writing during that **Discovery Period** shall be deemed first made during the **Policy Period**.

### **Employee**

A natural person under a contract of employment with a **Company**.

**Employee** does not include any:

- (i) principal, partner, director or officer; or
- (ii) temporary contract labourer, self employed person or labour-only sub-contractor.

### **Full Annual Premium**

The **Premium** plus any additional premium (as annualised) charged for any endorsements applied to this policy during the **Policy Period**.

### **General Terms and Conditions**

This policy's General Terms and Conditions

## **Insurer**

As specified in the schedule

## **Policy Aggregate Limit of Liability**

The amount specified under Policy Aggregate Limit of Liability in the schedule.

## **Policy Period**

The period of time from the inception date specified in the schedule to the expiry date specified in the schedule or, if earlier, to the date of cancellation of this policy.

## **Policyholder**

The entity specified under Policyholder in the schedule.

## **Pollutants**

Any solid, liquid, biological, radiological, gaseous or thermal irritant or containment whether occurring naturally or otherwise, including asbestos, smoke, vapour, soot, fibres, mould, spores, fungus, germs, acids, alkalis, nuclear or radioactive material of any sort, chemicals or waste. Waste includes material to be recycled, reconditioned or reclaimed.

## **Premium**

The premium detailed under Premium in the schedule.

## **Purchased**

Shown in the schedule as purchased.

## **Responsible Officer**

Any Chief Executive Officer, Chief Financial Officer, Chief Compliance Officer, Chief Information Officer, Data Protection Officer, Chief Information Security Officer, Risk Manager, General Counsel or position equivalent to any of the foregoing.

## **Retention**

With respect to a **Coverage Section** or Cover, the amount or amounts specified in the schedule as its Retention.

## **Retroactive Date**

With respect to a **Coverage Section**, the date specified in the schedule as its Retroactive Date.

## **Single Insured Event**

Any one or more **Insured Events** to the extent that such **Insured Events** arise out of, are based upon, are in connection with, or are otherwise attributable to the same originating cause or source. All such **Insured Events** shall be regarded as a **Single Insured Event** regardless of whether such **Insured Events** involve the same or different claimants, **Insureds** or causes of action.

## **Subsidiary**

Any entity of which the **Policyholder** has or had **Control** on or before the inception date specified in the schedule either directly or indirectly through one or more of its other **Subsidiaries**.

**Subsidiary** shall also automatically include any entity of which the **Policyholder** acquires **Control**, either directly or indirectly through one or more of its other **Subsidiaries** during the **Policy Period**, provided that such acquired entity:

- (i) undertakes materially similar or identical business activities to the acquiring **Company**;
- (ii) has no prior claims or losses that could otherwise be covered under this policy;
- (iii) has total gross revenues that are less than 10% of the total gross revenue of the **Policyholder**; and
- (iv) has less than 50% of their total revenue from the United States of America.

For the purposes of this definition "**Control**" means where the **Policyholder**:

- (a) controls the election of the majority of the board of directors of such entity;
- (b) controls more than half of the voting power of such entity; or
- (c) holds more than 50% of the issued share / equity capital of such entity.

Cover under this policy for such entities which the **Policyholder** has acquired **Control**, either directly or indirectly through one or more of its other **Subsidiaries** during the **Policy Period**, shall only apply to **Claims** made or other **Insured Events** first occurring on or after the date of acquisition.

The applicable **Retroactive Date** and **Continuity Date** in respect of each such entity shall be the date on which the **Policyholder** acquired **Control** of the entity.

### **Third Party**

Any entity or natural person except:

- (i) any **Insured**; and
- (ii) any other entity or natural person having a financial interest or executive role in the operation of a **Company**.

## **10. Exclusions**

---

The following Exclusions apply to all **Coverage Sections** and in addition to the Exclusions set out in each **Coverage Section**.

### **10.1. Conduct**

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

- (i) any wilful disregard or non-compliance with a ruling, direction or injunction by a court, tribunal, arbitrator or a **Regulator** within the relevant jurisdiction;
- (ii) the committing of any dishonest, fraudulent, criminal, reckless or malicious act, error or omission, or any intentional or knowing violation of the law, if committed by:
  - (a) any director, principal, partner or **Responsible Officer** of a **Company**, whether acting on their own or in collusion with others; or
  - (b) any **Employee** acting in collusion with any of a **Company's** directors, principals, partners or **Responsible Officers**.

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

## 10.2. Natural Disaster

The **Insurer** shall not be liable for **Loss**, arising out of, based upon, or attributable to any fire, smoke, explosion, lightening, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, Act of God or any natural event howsoever caused.

## 10.3. Pollution

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

- (i) the actual, alleged or threatened discharge, dispersal, seepage, release, migration or escape of **Pollutants**;
- (ii) any direction, request or effort to test for, monitor, clean up, remove, contain, treat, detoxify or neutralise **Pollutants** or respond to or assess the effects of **Pollutants**; or
- (iii) any actual or alleged act, error or omission in any way connected to **Pollutants**.

## 10.4. Prior Claims and Circumstances

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

- (i) any circumstance or **Insured Event** that as of the inception date specified in the schedule may reasonably have been expected by a **Company's Responsible Officer** to give rise to a claim under this policy; or any circumstance or **Insured Event** of which notice has been given under any policy of which this policy is a renewal or replacement or which it may succeed in time;
- (ii) any pending or prior civil, criminal, administrative or regulatory proceeding, investigation, arbitration, mediation, other dispute resolution or adjudication of which a **Company's Responsible Officer** had notice as of the **Continuity Date**, or alleging or deriving from the same or essentially the same facts alleged in such actions; or
- (iii) any **Insured Event** that would otherwise constitute a **Single Insured Event** with any claim or other matter reported under any policy of which this policy is a renewal or a replacement or which it may succeed in time.

## 10.5. Satellite Failure

The **Insurer** shall not be liable for **Loss**, arising out of, based upon, or attributable to any satellite failure.

## 10.6. Monetary Value

The **Insurer** shall not be liable for **Loss** consisting of the actual monetary value of cash or a monetary instrument (including cryptocurrencies) arising from:

- (i) the theft of such cash or monetary instrument (including cryptocurrencies) from an **Insured**; or
- (ii) the transfer or loss of such cash or monetary instrument (including cryptocurrencies) from or to an **Insured's** accounts or accounts under an **Insured's** control, including customer accounts. Accounts includes deposit, credit, debit, prepaid and securities brokerage accounts.

## 10.7. Sanctions

The **Insurer** shall not be deemed to provide cover and the **Insurer** shall not be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose the **Insurer**, its parent company or its ultimate controlling entity to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, the United Kingdom or the United States of America.

## 10.8. Taxes

The **Insurer** shall not be liable for **Loss** arising out of, based upon, or attributable to, or consisting of, any taxes payable by a **Company** howsoever arising, other than any VAT or equivalent taxes payable in connection with the provision of covered **IT Services, Legal Services, Reputation Protection Services, Notification Action, Credit Monitoring and ID Monitoring Services** or **Cyber Extortion Services**.

#### 10.9. Uninsurable and Prohibited Loss

The **Insurer** shall not be liable for **Loss**:

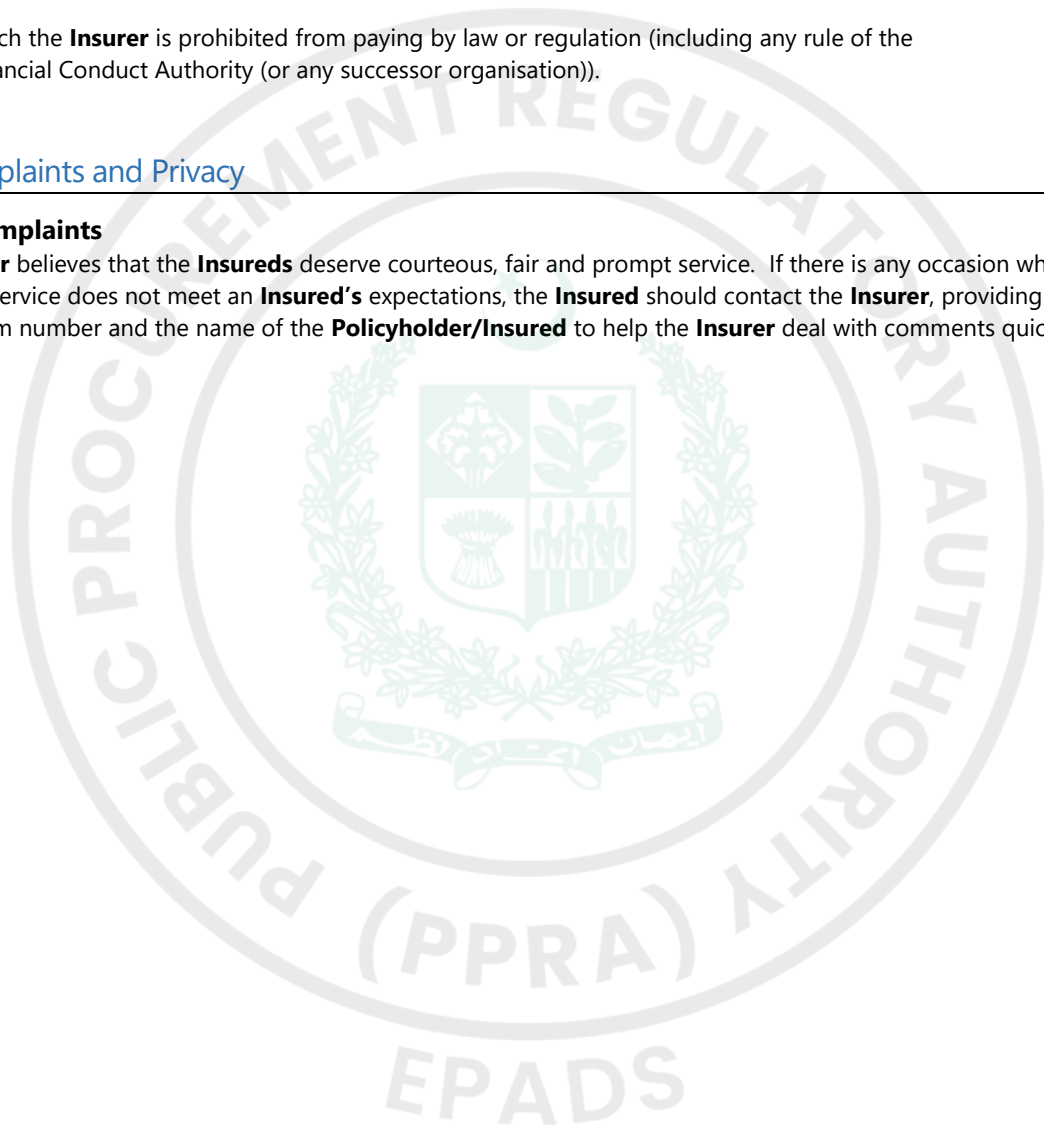
- (i) which is uninsurable under the law of this policy or the law of the jurisdiction where the **Claim** is first made or other **Insured Event** first occurs; or
- (ii) which the **Insurer** is prohibited from paying by law or regulation (including any rule of the Financial Conduct Authority (or any successor organisation)).

### 11. Complaints and Privacy

---

#### 11.1. Complaints

The **Insurer** believes that the **Insureds** deserve courteous, fair and prompt service. If there is any occasion when the **Insurer's** service does not meet an **Insured's** expectations, the **Insured** should contact the **Insurer**, providing the policy/claim number and the name of the **Policyholder/Insured** to help the **Insurer** deal with comments quickly.



# Network Interruption Coverage

## 1. Insurance Covers

---

### 1.1. Network Interruption Loss

The **Insurer** will, with regard to an **Insured Event** which first occurs during the **Policy Period**, pay to each **Company**:

- (i) **Network Loss** which results from the **Insured Event** and which the **Company** incurs during the **Insured Event** (but, if the **Insured Event** lasts longer than 120 days, only during the first 120 days); and
- (ii) **Network Loss** which results from the **Insured Event** and which the **Company** incurs during the 90 days following resolution of the **Insured Event**.

### 1.2. Interruption and Mitigation Costs

The **Insurer** will pay, to or on behalf of each **Company**, **Network Interruption Costs** incurred in mitigating the impact of an **Insured Event** which first occurs during the **Policy Period**.

### 1.3. Loss Preparation Costs

If **Loss Preparation Costs** Cover is **Purchased**, the **Insurer** will pay, to or on behalf of each **Company**, **Loss Preparation Costs** incurred as a result of an **Insured Event** which first occurs during the **Policy Period**.

## 2. Definitions

---

The following definitions are specific to this **Network Interruption Coverage Section**. All other definitions set out within Section 10 (Definitions) of the **General Terms and Conditions** shall apply as stated.

### Company Computer System

- (i) Any computer hardware, software or any other components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a **Company**; or
- (ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system.

### Cyber Terrorism

The premeditated use of disruptive activities against a **Company Computer System** or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

**Cyber Terrorism** does not include any such activities which are part of or in support of any use of military force or war.

### Increased Costs of Working

Expenses (including overtime of **Employees**) incurred over and above normal operating expenses in order to ensure continuation of the normal business operations of a **Company** and to reduce its loss of business income.

### Insured

A **Company**.

## Insured Event

- (i) If **Security Failure** Cover is **Purchased**, a **Material Interruption** to a **Company Computer System** that is caused by a **Security Failure**;
- (ii) if **System Failure** Cover is **Purchased**, a **Material Interruption** to a **Company Computer System** that is caused by a **System Failure**;
- (iii) if **Voluntary Shutdown** Cover is **Purchased**, a **Material Interruption** to a **Company Computer System** that is caused by a **Voluntary Shutdown**;
- (iv) if **OSP Security Failure** Cover is **Purchased**, a **Material Interruption** to an **OSP Computer System** that is caused by an **OSP Security Failure**; and
- (v) if **OSP System Failure** Cover is **Purchased**, a **Material Interruption** to an **OSP Computer System** that is caused by an **OSP System Failure**,

and in each case, only where the duration of the **Material Interruption** exceeds the applicable **Waiting Hours Period** specified in the schedule. For the avoidance of doubt, once the **Waiting Hours Period** has been exceeded the **Insurer** will be liable to pay **Network Loss** incurred during as well as after the **Waiting Hours Period**, subject to the **Retention** set out in the **Schedule**.

## Loss

- (i) For the purposes of Insurance Cover 1.1, **Network Loss**;
- (ii) for the purposes of Insurance Cover 1.2, **Network Interruption Costs**;
- (iii) for the purposes of Insurance Cover 1.3, **Loss Preparation Costs**.

## Loss Preparation Costs

Reasonable and necessary professional fees and expenses incurred by a **Company** with the **Insurer's** consent, for the services of a third-party forensic accounting firm to establish, prove, verify or quantify **Network Loss** or **Network Interruption Costs** or prepare the proof of loss referred to in Condition 4.1 of this **Network Interruption Coverage Section**.

**Loss Preparation Costs** does not include any fees or expenses for consultation on coverage or negotiation of claims.

## Material Interruption

- (i) The suspension or degradation of a **Company Computer System** (for the purposes of Insured Event (i) – (iii)) or an **OSP Computer System** (for the purposes of Insured Event (iv) or (v)) causing the **Company** to be unable to continue the normal business operations of the **Company**; or
- (ii) the deletion, damage, corruption, alteration or loss of or to **Data** on a **Company Computer System** (for the purposes of Insured Event (i) – (iii)) or an **OSP Computer System** (for the purposes of Insured Event (iv) or (v)) causing the **Company** to be unable to access that **Data** and unable to continue the normal business operations of the **Company**.

## Network Interruption Costs

The reasonable and necessary costs and expenses that a **Company** incurs to minimise the **Network Loss**, or reduce the impact of a **Material Interruption**; provided however that the amount of **Network Loss** prevented or reduced would be greater than the costs and expenses incurred.

## Network Loss

- (i) A **Company's** actual loss sustained resulting from the reduction in business income calculated by taking either Network Loss Option 1 or Network Loss Option 2; and
- (ii) the **Company's Increased Costs of Working** (but only up to an amount equal to the reduction in business income that would have been incurred had the **Company** been unable to continue its normal operating procedure).

Network Loss Option 1 (Net Profit and Continuing Fixed Costs Calculation) is calculated as follows:

Take the net profit or loss which would have been earned or incurred had the **Material Interruption** not occurred and add the costs (including ordinary payroll) which necessarily continue during the **Material Interruption**.

Network Loss Option 2 (Gross Profits Calculation) is calculated as follows:

Take the revenue which would have been derived from the operation of the business had the **Material Interruption** not occurred and subtract the variable costs, and any other costs, which do not necessarily continue during the **Material Interruption**.

## OSP Computer System

Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by an **Outsource Service Provider**.

## OSP Security Failure

Any intrusion of, unauthorised access (including any unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) an **OSP Computer System**, including that which results in or fails to mitigate any:

- (i) denial of service attack or denial of access; or
- (ii) receipt or transmission of a malicious code, malicious software or virus.

## OSP System Failure

Any unintentional and unplanned outage of an **OSP Computer System** such that the **Outsource Service Provider** is unable to provide to a **Company** the services described in a contract between a **Company** and an **Outsource Service Provider** pursuant to which an **Outsource Service Provider** provides services to a **Company** for a fee.

## Outsource Service Provider

A **Third Party** that a **Company** has appointed to provide specified information technology services (such as the processing, hosting and storage of **Data**) based on an express contractual agreement, but only to the extent of the provision of such services.

**Outsource Service Provider** does not include:

- (i) a public utility (including a provider of electricity, gas, water or telecommunication services);
- (ii) an internet service provider (including any provider of internet connectivity); or,
- (iii) a securities exchange or market.

## Security Failure

- (i) Any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a **Company Computer System**, including that which results in or fails to mitigate any:
  - (a) denial of service attack or denial of access; or,
  - (b) receipt or transmission of a malicious code, malicious software or virus; or
- (ii) the unauthorised reprogramming or corruption of software (including firmware) which renders a **Company Computer System** or any component thereof non-functional or useless for its intended purpose.

### **System Failure**

Any unintentional and unplanned outage of a **Company Computer System**.

### **Voluntary Shutdown**

A voluntary and intentional shutdown or impairment of a **Company Computer System** by or at the direction of:

- (i) the Chief Information officer or Chief Information Security Officer of a **Company** (or the equivalent position regardless of title) who has at least 5 years' experience in an Information Security or Technology role; or
- (ii) an information technology services firm appointed by a **Company** that has been approved in advance of such appointment by the **Insurer**,

after the discovery of a **Security Failure**, with the reasonable belief that such shutdown or impairment would limit the **Loss** that would otherwise be incurred as a result of that **Security Failure**.

### **Waiting Hours Period**

The number of hours as defined in the schedule, commencing at the beginning of a **Material Interruption**.

## **3. Exclusions**

---

The following Exclusions are specific to this **Network Interruption Coverage Section**. They apply in addition to the Exclusions in Section 11 (Exclusions) of the **General Terms and Conditions**.

The **Insurer** shall not be liable for **Loss**:

### **3.1. Betterment**

Consisting of the costs of:

- (i) updating, upgrading, enhancing or replacing any component of a **Company Computer System** or an **OSP Computer System** to a level beyond that which existed prior to the occurrence of a **Material Interruption**; however, this exclusion shall not apply to the extent that the replacement of a component of a **Company Computer System** is:
  - (a) required to end the **Material Interruption**; and
  - (b) no longer available and can only be reasonably replaced with an upgraded or enhanced version.
- (ii) removing software program errors or vulnerabilities.

### **3.2. Bodily Injury and Property Damage**

Arising out of, based upon or attributable to any:

- (i) physical injury, mental illness, sickness, disease or death; or

(ii) loss, damage or destruction of tangible property.

### 3.3. Business Conditions

Consisting of loss of earnings, or costs or expenses, attributable to unfavourable business conditions.

### 3.4. Government Entity or Public Authority

Arising out of, based upon or attributable to any seizure, confiscation or nationalisation of a **Company Computer System** by order of any government entity or public authority.

### 3.5. Infrastructure

Arising out of, based upon or attributable to any electrical or mechanical failure of infrastructure not under the control of a **Company** (or, where **OSP Security Failure** Cover or **OSP System Failure** Cover is **Purchased**, an **Outsource Service Provider**), including any electrical power interruption, surge, brownout or blackout, failure of telephone lines, data transmission lines, or other telecommunications or networking infrastructure.

### 3.6. Liability

Arising out of, based upon or attributable to any:

- (i) written demand, civil, administrative or arbitral proceedings, made by any **Third Parties** seeking any legal remedy; or
- (ii) penalties paid to **Third Parties**.

### 3.7. Patent

Arising out of, based upon or attributable to any infringement of patents.

### 3.8. Trading Losses

Consisting of trading losses, liabilities or changes in trading account value.

### 3.9. War and Terrorism

Arising out of, based upon or attributable to any war (whether war is declared or not), terrorism (except **Cyber Terrorism**), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

## 4. Conditions

---

The following conditions are specific to this **Network Interruption Coverage Section** and shall apply in addition to the conditions set out within the **General Terms and Conditions**.

### 4.1. Proof of Loss

In addition to the requirements to give notice to the **Insurer** under Section 8.1 (Notice and Reporting) of the **General Terms and Conditions**, and before coverage under this **Network Interruption Coverage Section** shall apply, a **Company** must also:

- (i) complete and sign a written, detailed and affirmed proof of loss after the resolution of the **Material Interruption**, which will include:
  - (a) a full description of the **Network Interruption Costs** or **Network Loss** and the circumstances of such **Network Interruption Costs** or **Network Loss**;

- (b) a detailed calculation of any **Network Loss**;
  - (c) all underlying documents and materials that reasonably relate to or form a part of the basis of the proof of the **Network Interruption Costs** or **Network Loss**; and
- (ii) upon the **Insurer's** request promptly respond to requests for information.

All adjusted claims are due and payable 45 days after:

- a. the presentation of the satisfactory written proof of **Network Loss** and **Network Interruption Costs** as provided for in (i) and (ii) above; and
- b. the subsequent written acceptance thereof by the **Insurer**.

**Network Loss** shall be reduced by any amounts recovered by a **Company** (including the value of any service credits provided to a **Company**) from any party (including any **Outsource Service Provider**).

The costs and expenses of establishing or proving **Network Loss** and/or **Network Interruption Costs** under this **Network Interruption Coverage Section**, including those associated with preparing the proof of loss, shall be the obligation of the **Company** and are not covered under this policy except as covered under 1.3 (Loss Preparation Costs) of this **Network Interruption Coverage Section**.

#### 4.2. Appraisal

If a **Company** and the **Insurer** disagree on the extent of **Network Loss** or **Network Interruption Costs**, either may make a written demand for an appraisal of such **Network Loss** or **Network Interruption Costs**. 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 10 years' standing and who is a partner in a major international accounting firm, experienced in assessing loss of this nature. Each appraiser will separately state the extent of **Network Loss** or **Network Interruption Costs**. 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 costs, including the costs of their respective chosen appraiser, and
- (ii) bear the expenses of the expert equally.

# Cyber Extortion Coverage

## 1. Insurance Covers

---

### 1.1 Cyber Extortion

The **Insurer** will pay to each **Company**, **Loss** that the **Company** incurs solely as a result of an **Extortion Threat** which first occurs during the **Policy Period**.

## 2. Definitions

---

The following definitions are specific to this **Cyber Extortion Coverage Section**. All other definitions set out within Section 10 (Definitions) of the **General Terms and Conditions** shall apply as stated.

### Breach of Confidential Information

The unauthorised disclosure or transmission of **Confidential Information**.

### Company Computer System

- (i) Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a **Company**;
- (ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system; or
- (iii) any employee "Bring Your Own Device" but only to the extent such device is used to access any of the foregoing computer hardware, software or components thereof or **Data** contained therein.

### Confidential Information

**Corporate Information** and **Personal Information** in a **Company's** or **Information Holder's** care, custody or control or for which a **Company** is legally responsible.

### Corporate Information

A **Third Party's** items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

### Cyber Extortion Expenses

The reasonable and necessary fees, costs and expenses of any firm appointed by the **Insurer** or any other firm appointed by the **Company** that has been approved by the **Insurer** in advance of such appointment to provide the **Cyber Extortion Services**.

### Cyber Extortion Services

- (i) Conducting an investigation to determine the validity, cause and scope of an **Extortion Threat**;
- (ii) advising on the response to an **Extortion Threat**;
- (iii) containing or resolving the disruption of the operations of a **Company Computer System** caused by the **Extortion Threat**; or
- (iv) assisting a **Company** in negotiating a resolution to an **Extortion Threat**.

### Cyber Terrorism

The premeditated use of disruptive activities against a **Company Computer System** or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

**Cyber Terrorism** does not include any such activities which are part of or in support of any use of military force or war.

### **Extortion Threat**

Any threat or connected series of threats, for the purpose of demanding money, securities or other tangible or intangible property of value from a **Company**, to:

- (i) commit or continue a **Breach of Confidential Information**;
- (ii) commit or continue an intentional attack against a **Company Computer System** (including through the use of ransomware); or
- (iii) disclose information concerning a vulnerability in a **Company Computer System**.

### **Information Holder**

A **Third Party** that:

- (i) a **Company** has provided **Personal Information** or **Corporate Information** to; or
- (ii) has received **Personal Information** or **Corporate Information** on behalf of a **Company**.

### **Insured**

A **Company**.

### **Insured Event**

An **Extortion Threat**.

### **Loss**

- (i) Any payment of cash, monetary instrument, cryptocurrencies (including the costs to obtain such cryptocurrencies) or the fair market value of any property which a **Company** has paid, to prevent or end an **Extortion Threat**; and
- (ii) **Cyber Extortion Expenses**.

### **Personal Information**

Any **Data** relating to an identified or identifiable natural person.

**Personal Information** includes a natural person's name, online identifiers, telephone number, credit card or debit card number, account and other banking information, medical information, or any other information about a natural person protected under any **Data Protection Legislation**.

## **3. Exclusions**

The following Exclusions are specific to this **Cyber Extortion Coverage Section**. They apply in addition to the Exclusions in Section 11 (Exclusions) of the **General Terms and Conditions**.

The **Insurer** shall not be liable for any **Loss**:

### **Anti-terrorism legislation**

To the extent that the provision of such payment to or on behalf of a **Company** would expose the **Insurer**, its parent company or its ultimate controlling entity to any applicable anti-terrorism legislation or regulation under United Nations resolutions laws or regulations of the European Union, or the United States of America or the United Kingdom.

### **Bodily Injury and Property Damage**

For any:

- (i) physical injury, mental illness, sickness, disease or death; or
- (ii) loss, damage or destruction of tangible property.

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

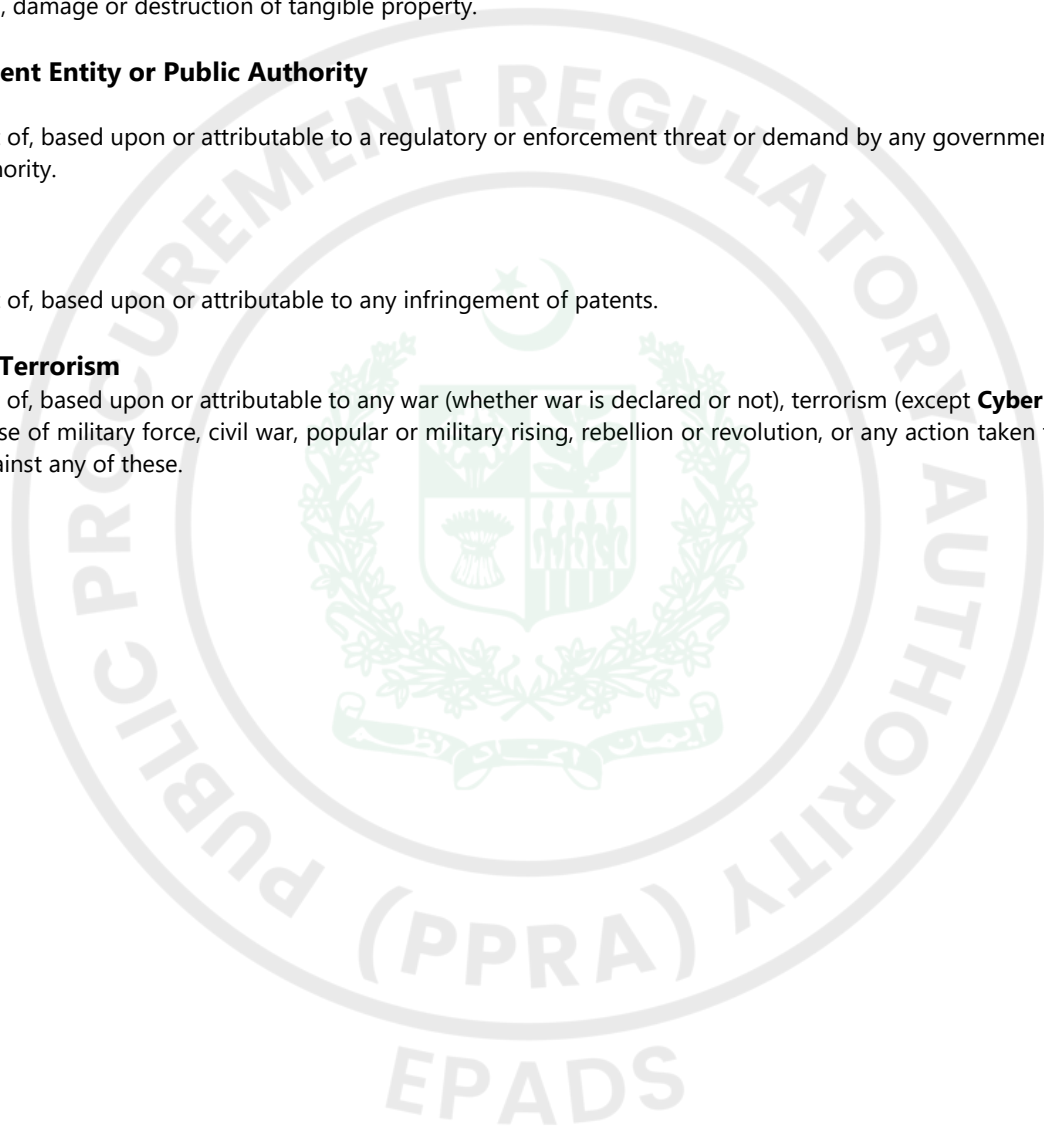
Arising out of, based upon or attributable to a regulatory or enforcement threat or demand by any government entity or public authority.

### **Patent**

Arising out of, based upon or attributable to any infringement of patents.

### **War and Terrorism**

Arising out of, based upon or attributable to any war (whether war is declared or not), terrorism (except **Cyber Terrorism**), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these.



# Event Management Coverage

## 1. Insurance Covers

---

### 1.1. Event Management

The **Insurer** will pay to or on behalf of each **Company**:

- (iii) **Legal Expenses;**
- (iv) **IT Expenses;**
- (v) **Data Recovery Expenses;**
- (vi) **Reputation Protection Expenses;**
- (vii) **Notification Expenses;**
- (viii) **Credit Monitoring and ID Monitoring Expenses;** and
- (ix) (if First Response Cover is **Purchased**) **First Response Expenses,**

incurred solely as a result of an **Insured Event** which has occurred, or the **Company** reasonably believes has occurred, before or during the **Policy Period** and which, during the **Policy Period**, the **Company** first becomes aware of such **Insured Event**.

**First Response Expenses** will only be paid by the **Insurer** to the extent that they are incurred during the period of hours stated for the First Response Cover in the schedule, which shall commence when the **Responsible Officer** of the **Policyholder** first notifies the **First Response Advisor** of the **Insured Event** by contacting the Emergency Number specified in the schedule.

No **Retention** shall apply to **First Response Expenses**.

## 2. Definitions

---

The following definitions are specific to this **Event Management Coverage Section**. All other definitions set out within Section 10 (Definitions) of the **General Terms and Conditions** shall apply as stated.

### **Breach of Confidential Information**

The unauthorised disclosure or transmission of **Confidential Information**.

### **Company Computer System**

- (x) Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a **Company**;
- (xi) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system; or
- (xii) any employee "Bring Your Own Device" but only to the extent such device is used to access any of the foregoing computer hardware, software or components thereof or **Data** contained therein.

### **Confidential Information**

**Corporate Information** and **Personal Information** in a **Company's** or **Information Holder's** care, custody or control or for which a **Company** is legally responsible.

## Corporate Information

A **Third Party's** items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

## Credit Monitoring and ID Monitoring Expenses

The reasonable and necessary fees, costs and expenses incurred by a **Company**, with the **Insurer's** prior written consent, for **Credit Monitoring and ID Monitoring Services** provided to those **Data Subjects** whose **Confidential Information** is reasonably believed to have been disclosed or transmitted.

## Credit Monitoring and ID Monitoring Services

Credit or identity theft monitoring services to identify possible misuse of any **Personal Information** as a result of an actual or suspected **Breach of Confidential Information**.

## Cyber Terrorism

The premeditated use of disruptive activities against a **Company Computer System** or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

**Cyber Terrorism** does not include any such activities which are part of or in support of any use of military force or war.

## Data Recovery Expenses

The reasonable and necessary fees, costs and expenses incurred by a **Company** on actions taken to:

- (i) identify lost, damaged, destroyed or corrupted **Data**;
- (ii) determine whether any lost, damaged, destroyed or corrupted **Data** can be restored, repaired, recollected or recreated; and
- (iii) restore, recreate, repair or recollect lost, damaged, destroyed or corrupted **Data** to substantially the form in which it existed immediately prior to the **Insured Event**, including where necessary the cost to restore **Data** from backups or the recreation of **Data** from physical records.

## Data Subject

Any natural person whose **Personal Information** has been either collected, stored or processed by or on behalf of a **Company**.

## First Response Advisor

The law firm specified in the schedule, or other law firms instructed by such specified law firm, or any replacement firm nominated by the **Insurer** in the event of a conflict of interest, with respect to whom a **Company** shall enter into a **Relevant Engagement**.

## First Response Expenses

The reasonable and necessary fees, costs and expenses of:

2. the **First Response Advisor** providing **First Response Legal Services**;
3. the **First Response IT Specialist** providing **IT Services**; and

4. the **Public Relations Advisor**, if its appointment is considered necessary by the **First Response Advisor** or the **Insurer**, providing **Reputation Protection Services**.

#### **First Response IT Specialists**

The firm specified in the schedule, or any replacement firm appointed by the **Insurer** in the event of a conflict of interest.

#### **First Response Legal Services**

- (ii) legal advice and support provided pursuant to a **Relevant Engagement**;
- (iii) coordinating the **First Response IT Specialist**, and, if considered necessary by the **First Response Advisor** or **Insurer**, the **Public Relations Advisor**; and
- (iv) preparation and notification to any relevant **Regulator**.

#### **Information Holder**

A **Third Party** that:

- (i) a **Company** has provided **Personal Information** or **Corporate Information** to; or
- (ii) has received **Personal Information** or **Corporate Information** on behalf of a **Company**.

#### **Insured**

A **Company**.

#### **Insured Event**

- (xiii) A **Breach of Confidential Information**;
- (xiv) a **Security Failure**; or
- (xv) in respect of **Data Recovery Expenses** only, an **Operational Failure**.

#### **IT Expenses**

The reasonable and necessary fees, costs and expenses of an **IT Specialist** providing **IT Services**.

#### **IT Services**

The services of:

- (i) substantiating whether an **Insured Event** has occurred, how it occurred and whether it is still occurring;
- (ii) identifying any compromised **Data** resulting from an **Insured Event**;
- (iii) establishing the extent to which **Confidential Information** may have been compromised; or
- (iv) containing and resolving an **Insured Event** and making recommendations to prevent or mitigate a future occurrence of the same or similar event.

#### **IT Specialist**

An information technology services firm appointed by a **Company** that has been approved in advance of such appointment by the **Insurer**.

#### **Legal Expenses**

The reasonable and necessary fees, costs and expenses of a **Response Advisor** providing the **Legal Services**.

### **Legal Services**

The services of:

- (i) co-ordinating the **IT Specialist** or **Public Relations Advisor**;
- (ii) advising, notifying and corresponding on any notification requirements with any relevant **Regulator**; or
- (iii) monitoring complaints raised by **Data Subjects** and advising a **Company** on responses to an **Insured Event** for the purposes of minimising harm to the **Company**, including actions taken to maintain and restore public confidence in the **Company**,

in dealing with any actual or suspected **Breach of Confidential Information** or **Security Failure**.

### **Loss**

**Legal Expenses, IT Expenses, Data Recovery Expenses, Reputation Protection Expenses, Notification Expenses, Credit Monitoring and ID Monitoring Expenses and First Response Expenses.**

### **Notification**

- (i) Setting up and operating call centres;
- (ii) preparing and notifying;
  - (a) those **Data Subjects** whose **Confidential Information** is reasonably believed to have been disclosed or transmitted; or
  - (b) any relevant **Regulator**; or
- (iii) investigating and collating information,

with regard to any actual or suspected **Breach of Confidential Information**.

### **Notification Expenses**

The reasonable and necessary fees, costs and expenses incurred by a **Company** on **Notification**.

### **Operational Failure**

The loss or damage to **Data** caused by:

- (i) a negligent or unintentional act or failure to act by:
  - (a) an **Insured**;
  - (b) an employee of an **Insured**; or
  - (c) a third party service provider to an **Insured**;
- (ii) the loss or theft of electronic equipment; or
- (iii) a magnetic event other than:
  - (a) the use of electromagnetic or directed-energy weapons; or

- (b) the natural deterioration of the storage media or data.

### **Personal Information**

Any information relating to an identified or identifiable natural person.

**Personal Information** includes a natural person's name, online identifier, telephone number, credit card or debit card number, account and other banking information, medical information, or any other information about a natural person protected under any **Data Protection Regulation**.

### **Public Relations Advisor**

A consultant appointed by the **Insurer** or the **Response Advisor**, or any other consultant appointed by a **Company** that has been approved by the **Insurer** in advance of such appointment, to provide **Reputation Protection Services**.

### **Regulator**

A regulator established pursuant to **Data Protection Legislation** in any jurisdiction and which is authorised to enforce statutory obligations in relation to the collecting, storing, processing or control of **Confidential Information**.

**Regulator** includes any other government agency or authorised data protection authority who makes a demand on a **Company** in relation to **Data Protection Legislation**.

### **Relevant Engagement**

A written agreement between the **First Response Advisor** and a **Company** governing the provision of the **First Response Legal Services** to the **Company**.

### **Reputation Protection Expenses**

The reasonable and necessary fees, costs and expenses of a **Public Relations Advisor** providing **Reputation Protection Services**.

### **Reputation Protection Services**

Advice and support (including advice concerning media strategy and independent public relations services, and the design and management of a communications strategy) in order to mitigate or prevent the potential adverse effect, or reputational damage, from media reporting of an **Insured Event**.

### **Response Advisor**

Any law firm appointed by the **Insurer**, or any other law firm appointed by a **Company** that has been approved in advance of such appointment by the **Insurer**.

### **Security Failure**

- (xvi) Any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a **Company Computer System**, including that which results in or fails to mitigate any:
- (a) denial of service attack or denial of access; or
  - (b) receipt or transmission of a malicious code, malicious software or virus;
- (xvii) The loss of **Data** arising from the physical theft or loss of hardware controlled by a **Company**; or
- (xviii) the unauthorised reprogramming or corruption of software (including firmware) which renders a **Company Computer System** or any component thereof non-functional or useless for its intended purpose.

### 3. Exclusions

---

The following Exclusions are specific to this **Event Management Coverage Section**. They apply in addition to the Exclusions in Section 11 (Exclusions) of the **General Terms and Conditions**.

The **Insurer** shall not be liable for any **Loss**:

#### 3.1. Betterment

Consisting of the costs of:

- (i) updating, upgrading, enhancing or replacing a **Company Computer System** to a level beyond that which existed prior to the occurrence of an **Insured Event**; and
- (ii) removing software program errors or vulnerabilities.

#### 3.2. Bodily Injury and Property Damage

Arising out of, based upon or attributable to any:

- (i) physical injury, mental illness, sickness, disease or death; or
- (ii) loss, damage or destruction of tangible property.

#### 3.3. Government Entity or Public Authority

Arising out of, based upon or attributable to any seizure, confiscation or nationalisation of a **Company Computer System** by order of any government entity or public authority.

#### 3.4. Infrastructure

Arising out of, based upon or attributable to any electrical or mechanical failure of infrastructure not under the control of a **Company**, including any electrical power interruption, surge, brownout or blackout, failure of telephone lines, data transmission lines, or other telecommunications or networking infrastructure.

This Exclusion 3.4 shall not apply to **Loss** arising out of, based upon or attributable solely to a **Security Failure** or **Breach of Confidential Information** that is caused by such electrical or mechanical failure of infrastructure.

#### 3.5. Internal/Staff Costs

Consisting of the costs of payroll, fees, benefits, overheads or internal charges of any kind incurred by a **Company**.

#### 3.6. Patent/Trade Secret

Arising out of, based upon or attributable to any:

- (i) infringement of patents;
- (ii) loss of rights to secure registration of patents; or
- (iii) misappropriation of trade secrets by or for the benefit of a **Company**.

#### 3.7. War and Terrorism

Arising out of, based upon or attributable to any war (whether war is declared or not), terrorism (except **Cyber Terrorism**), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

## 4. Conditions

---

The following conditions are specific to this **Event Management Coverage Section** and shall apply in addition to the conditions set out within the **General Terms and Conditions**.

### 4.1. First Response Notification

The cover provided for **First Response Expenses** is granted solely with respect to a **Breach of Confidential Information** or **Security Failure** first discovered during the **Policy Period** and a **Company** shall, as a condition precedent to the obligations of the **Insurer** in respect of such **First Response Expenses**, notify the **Insurer** by contacting the Emergency Number specified in the schedule as soon as reasonably practicable after the **Breach of Confidential Information** or **Security Failure** first occurs.



# Security and Privacy Liability Coverage

## 1. Insurance Covers

---

### 1.1 Data Protection Investigation and Data Protection Fines

The **Insurer** will pay, to or on behalf of each **Company**, **Loss** resulting from a **Regulatory Investigation** first occurring during the **Policy Period**.

### 1.2 Cyber Liability

The **Insurer** will pay, to or on behalf of each **Insured**, **Loss** resulting from a **Claim** first made during the **Policy Period** for any:

- (i) actual or alleged **Breach of Confidential Information** by an **Insured** or an **Information Holder**;
- (ii) actual or alleged **Security Failure**; or
- (iii) actual or alleged failure by a **Company** to notify a **Data Subject** or any **Regulator** of an unauthorised disclosure or transmission of **Personal Information** for which the **Company** is responsible in accordance with the requirements of any **Data Protection Legislation**,

which occurred or occurs prior to or during the **Policy Period**.

## 2. Definitions

---

The following definitions are specific to this **Security and Privacy Liability Coverage Section**. All other definitions set out within Section 10 (Definitions) of the **General Terms and Conditions** shall apply as stated.

### Breach of Confidential Information

The unauthorised disclosure or transmission of **Confidential Information**.

### Claim

- (i) A written demand against an **Insured**;
- (ii) civil, administrative or arbitral proceedings brought against an **Insured**; or
- (iii) a **PCI-DSS Assessment**,

seeking any legal remedy.

### Company Computer System

- (i) Any computer hardware, software or any components thereof that are linked together through a network of two or more devices accessible through the internet or an intranet or that are connected through data storage or other peripheral devices which are owned, operated, controlled or leased by a **Company**;
- (ii) any of the foregoing computer hardware, software or components thereof which is part of an industrial control system, including a supervisory control and data acquisition (SCADA) system;
- (iii) any employee "Bring Your Own Device" but only to the extent such device is used to access any of the foregoing computer hardware, software or components thereof or **Data** contained therein; or
- (iv) any cloud service or other hosted computer resources, used by a **Company** and operated by a **Third Party** service provider under a written contract between such **Third Party** service provider and a **Company**.

## Confidential Information

**Corporate Information** and **Personal Information** in a **Company's** or **Information Holder's** care, custody or control or for which a **Company** is legally responsible.

## Corporate Information

A **Third Party's** items of information that are not available to the public (including trade secrets, data, designs, forecasts, formulas, practices, processes, records, reports and documents) which are subject to contractual or legal protection.

## Cyber Terrorism

The premeditated use of disruptive activities against a **Company Computer System** or network, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

**Cyber Terrorism** does not include any such activities which are part of or in support of any use of military force or war.

## Damages

Damages that an **Insured** is legally liable to pay resulting from a **Claim** as ascertained by:

- (i) judgments or arbitral awards rendered against that **Insured**; or
- (ii) a settlement agreement negotiated by that **Insured** and which is approved by the **Insurer**.

**Damages** includes punitive or exemplary or multiple damages where lawfully insurable and any monetary amounts that an **Insured** is required by law or has agreed by settlement to deposit into a consumer redress fund.

## Data Protection Fines

Any lawfully insurable fines or penalties which are adjudicated by a **Regulator** to be payable by a **Company** for a breach of **Data Protection Legislation**.

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

## Data Protection Legislation

The Data Protection Act 1998, the Data Protection Act 2018 and the General Data Protection Regulation (Regulation (EU) 2016/679) and any subsequent legislation that alters, repeals or replaces such legislation and all other equivalent laws and regulations relating to the regulation and enforcement of data protection and data privacy in any country.

## Data Subject

Any natural person whose **Personal Information** has been either collected, stored or processed by or on behalf of a **Company**.

## Defence Costs

Reasonable and necessary legal fees, costs and expenses which an **Insured** incurs with the prior written consent of the **Insurer** in relation to the investigation, response, defence, appeal or settlement of a **Claim** or **Regulatory Investigation**, including court attendance costs incurred by or on behalf of that **Insured**.

**Defence Costs** does not include the remuneration of any **Insured**, cost of their time or any other costs or overheads of any **Insured**.

## Information Holder

A **Third Party** that:

- (i) a **Company** has provided **Personal Information** or **Corporate Information** to; or
- (ii) has received **Personal Information** or **Corporate Information** on behalf of a **Company**.

### **Insured**

- (i) A **Company**;
- (ii) a natural person who was, is or during the **Policy Period** becomes a principal, partner, director, officer or **Employee** of a **Company**;
- (iii) a natural person who is an independent contractor, temporary contract labourer, self-employed person, or labour-only sub-contractor, under the direction and direct supervision of a **Company** but only in relation to the services provided to that **Company**.

**Insured** includes the estate, heirs or legal representatives of a deceased, legally incompetent or bankrupt **Insured** referred to in (ii) above to the extent that a **Claim** is brought against them solely by reason of them having an interest in property that is sought to be recovered in a **Claim** against such **Insured** referred to in (ii) above.

### **Insured Event**

A **Claim** or a **Regulatory Investigation**.

### **Loss**

- (i) For the purposes of Insurance Cover 1.1, **Defence Costs** and **Data Protection Fines**;
- (ii) for the purposes of Insurance Cover 1.2, **Damages**, **Defence Costs** and any amounts payable in connection with a **PCI-DSS Assessment**.

**Loss** does not include:

- (a) non-compensatory or multiple damages (except to the extent covered as **Damages** or as part of a **PCI-DSS Assessment**) or liquidated damages;
- (b) fines or penalties (except **Data Protection Fines** to the extent covered in 1.1. (Data Protection Investigation and Data Protection Fines));
- (c) the costs and expenses of complying with any order for, grant of or agreement to provide injunctive or other non-monetary relief; or
- (d) an **Insured's** remuneration, cost of time or overheads.

### **PCI-DSS Assessment**

Any written demand received by a **Company** from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank or servicer processing payment card transactions (e.g., an "Acquiring Bank" or "Payment Processor") for a monetary amount (including fraud recovery, operational reimbursement, reimbursement of card reissuance costs and contractual fines and penalties) where:

- (i) a **Company** has contractually agreed to indemnify such Payment Card Association, bank or servicer processing payment card transactions for any monetary assessment made in connection with a **Company's** obligations under generally accepted and published Payment Card Industry Standards for data security, including such contractual obligations contained in a merchant services agreement or similar agreement; and
- (ii) such monetary assessment arises out of a **Breach of Confidential Information**.

## Personal Information

Any information relating to an identified or identifiable natural person.

**Personal Information** includes a natural person's name, online identifier, telephone number, credit card or debit card number, account and other banking information, medical information, or any other information about a natural person protected under any **Data Protection Legislation**.

## Regulator

A regulator established pursuant to **Data Protection Legislation** in any jurisdiction and which is authorised to enforce statutory obligations in relation to the collecting, storing, processing or control of **Confidential Information**.

**Regulator** includes any other government agency or authorised data protection authority who makes a demand on the **Insured** in relation to **Data Protection Legislation**.

## Regulatory Investigation

Any formal or official action, investigation, inquiry or audit by a **Regulator** against a **Company** once it is identified in writing by a **Regulator**, which arises out of the use or suspected misuse of **Personal Information** or any aspects of the control, collection, storing or processing of **Personal Information** or delegation of data processing to an **Information Holder**, which is regulated by **Data Protection Legislation**.

**Regulatory Investigation** does not include any industry-wide, non-firm specific, action, investigation, inquiry or audit.

## Security Failure

- (i) Any intrusion of, unauthorised access (including an unauthorised person using authorised credentials) to, or unauthorised use of (including by a person with authorised access) a **Company Computer System**, including that which results in or fails to mitigate any:
  - (a) denial of service attack or denial of access; or
  - (b) receipt or transmission of a malicious code, malicious software or virus;
- (ii) the loss of **Data** arising from the physical theft or loss of hardware controlled by a **Company**; or
- (iii) the unauthorised reprogramming or corruption of software (including firmware) which renders a **Company Computer System** or any component thereof non-functional or useless for its intended purpose.

## 3. Exclusions

---

The following Exclusions are specific to this **Security and Privacy Liability Coverage Section**. They apply in addition to the Exclusions in Section 11 (Exclusions) of the **General Terms and Conditions**.

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

### Anti-Trust

Any actual or alleged antitrust violation, restraint of trade, unfair competition or unfair or deceptive business practices, including violation of any consumer protection law.

This Exclusion 3.1 shall not apply to a **Regulatory Investigation** alleging such unfair competition directly in connection with a **Security Failure** or **Breach of Confidential Information**.

### Assumed Liability, Guarantee, Warranty

Any guarantee, warranty, contractual term or liability assumed or accepted by an **Insured** under any contract or agreement except to the extent such liability would have attached to the **Insured** in the absence of such contract or agreement.

This Exclusion 2.3 shall not apply to:

- (i) a contractual obligation to prevent a **Security Failure** or **Breach of Confidential Information**;
- (ii) an obligation under a confidentiality or disclosure agreement held within contracts with a **Third Party** to prevent a **Breach of Confidential Information**; or
- (iii) the obligation to comply with Payment Card Industry Data Security Standards.

### **Bodily Injury and Property Damage**

Any:

- (i) physical injury, mental illness, sickness, disease or death: however, this Exclusion 3.3 (i) shall not apply in respect of emotional distress or mental anguish arising solely out of an **Breach of Confidential Information**; or
- (ii) loss, damage or destruction of tangible property.

### **Employment Practices Liability**

Any of a **Company's** employment practices (including wrongful dismissal, discharge or termination, discrimination, harassment, retaliation or other employment-related claim).

This Exclusion 3.4 shall not apply to any **Claim** by an individual to the extent such individual is alleging:

- (i) a **Breach of Confidential Information** in connection with such individual's employment or application for employment with a **Company**; or
- (i) a failure to disclose a **Security Failure** or **Breach of Confidential Information**.

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

Any seizure, confiscation or nationalisation of a **Company Computer System** by order of any government entity or public authority.

### **Infrastructure**

Any electrical or mechanical failure of infrastructure not under the control of a **Company**, including any electrical power interruption, surge, brownout or blackout, failure of telephone lines, data transmission lines, or other telecommunications or networking infrastructure.

This Exclusion 3.6 shall not apply to **Loss** arising out of, based upon or attributable solely to a **Security Failure** or **Breach of Confidential Information** that is caused by such electrical or mechanical failure of infrastructure.

### **Insured v Insured**

Any **Claim** brought by or on behalf of an **Insured** against another **Insured**.

This Exclusion 3.7 shall not apply to an actual or alleged breach of **Personal Information** of any **Employee**, director, principal, partner or officer.

### **Patent/Trade Secret**

Any:

- (ii) infringement of patents;

- (iii) loss of rights to secure registration of patents; or
- (iv) misappropriation of trade secrets by or for the benefit of a **Company**.

### **PCI-DSS Assessment**

Any **PCI-DSS Assessment**, unless the specific **Insured** which is the subject of the **PCI-DSS Assessment** was validated as compliant with the generally accepted and published Payment Card Industry Standards for data security prior to and at the time of any **Breach of Confidential Information** which gives rise to such **PCI-DSS Assessment** occurring.

### **Securities Claims**

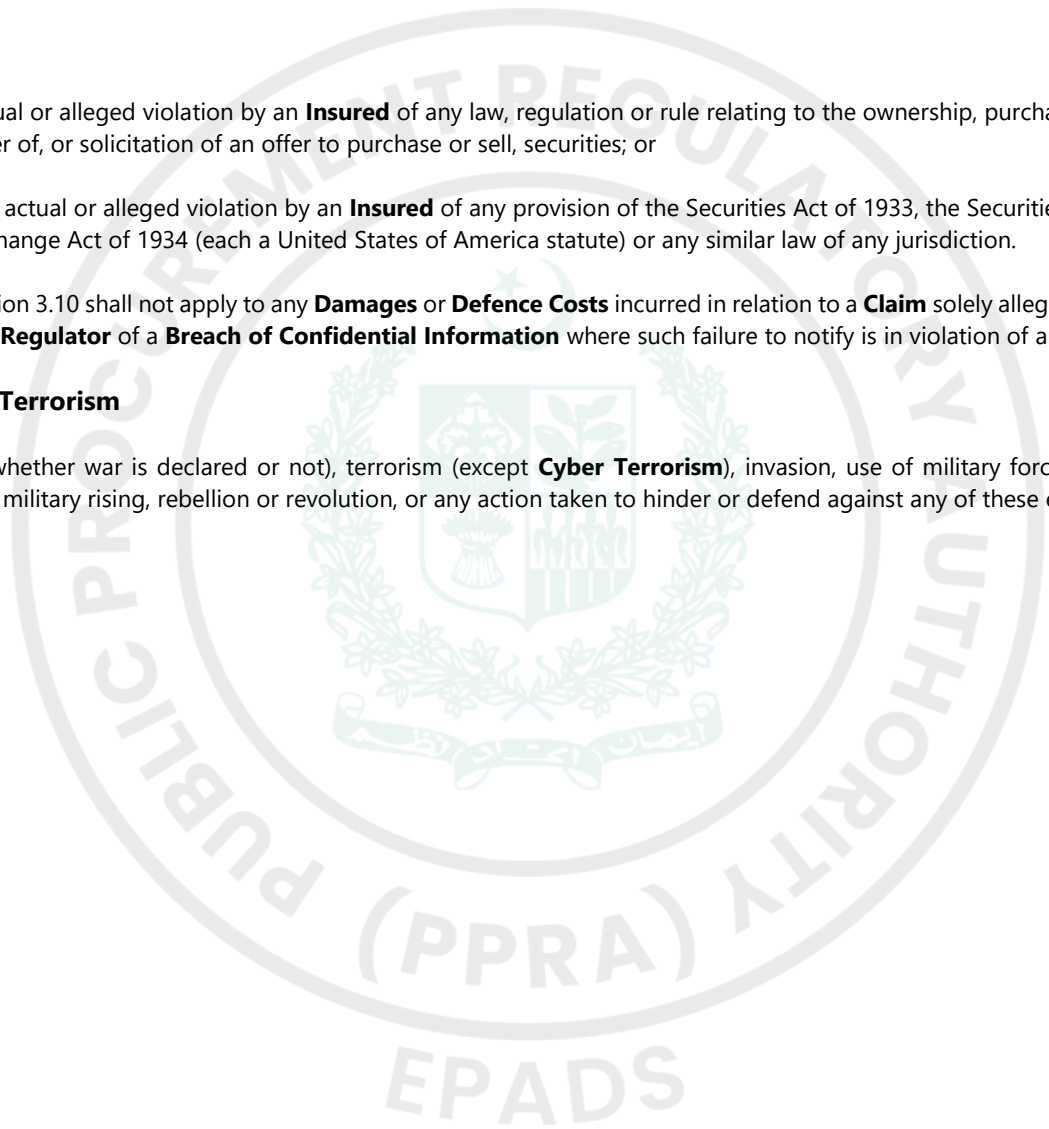
Any:

- (i) actual or alleged violation by an **Insured** of any law, regulation or rule relating to the ownership, purchase, sale or offer of, or solicitation of an offer to purchase or sell, securities; or
- (ii) any actual or alleged violation by an **Insured** of any provision of the Securities Act of 1933, the Securities Exchange Act of 1934 (each a United States of America statute) or any similar law of any jurisdiction.

This Exclusion 3.10 shall not apply to any **Damages** or **Defence Costs** incurred in relation to a **Claim** solely alleging a failure to notify a **Regulator** of a **Breach of Confidential Information** where such failure to notify is in violation of any law.

### **War and Terrorism**

Any war (whether war is declared or not), terrorism (except **Cyber Terrorism**), invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.



# Criminal Reward Fund Coverage

## 1. Insurance Covers

---

### Criminal Reward Fund

The **Insurer** may pay on a **Company's** behalf, at the **Insurer's** sole and absolute discretion, a **Criminal Reward Fund**.

## 2. Definitions

---

The following definitions are specific to this **Criminal Reward Fund Coverage Section**. All other definitions set out within Section 10 (Definitions) of the **General Terms and Conditions** shall apply as stated.

### Criminal Reward Fund

An amount offered by the **Insurer** for information that leads to the arrest and conviction of any individual(s) committing or trying to commit any illegal act related to the coverage under any of following **Coverage Sections** if such **Coverage Sections** are **Purchased: Security and Privacy Liability Coverage Section, Network Interruption Coverage Section, Event Management Coverage Section** and **Cyber Extortion Coverage Section**.

## 3. Exclusions

---

The following Exclusions are specific to this **Criminal Reward Fund Coverage Section**. They apply in addition to the Exclusions in Section 11 (Exclusions) of the **General Terms and Conditions** and in addition to the Exclusions set out within the **Data Protection and Cyber Liability Coverage Section, the Network Interruption Coverage Section, Event Management Coverage Section** and **Cyber Extortion Coverage Section**.

### 4.2 Fees, Costs and Expenses

The **Insurer** shall not be liable for **Loss** arising out of, based upon or attributable to any information provided by any **Insured**, an **Insured's** auditors, whether internal or external, any individual hired or retained to investigate the aforementioned illegal acts, or any other individuals with responsibilities for the supervision or management of the aforementioned individuals.

# Digital Media Content Liability

## Insurance Cover

---

### Digital Media Content Liability

The **Insurer** will pay, on behalf of each **Insured**, **Loss** resulting from a **Claim** first made during the **Policy Period** arising from **Digital Media Activities**.

## Definitions

---

The following definitions are specific to this **Digital Media Content Liability Coverage Section**. All other definitions set out within Section 10 (Definitions) of the **General Terms and Conditions** shall apply as stated.

### Claim

- (ii) A written demand against an **Insured**; or
- (iii) civil, administrative or arbitral proceedings brought against an **Insured**, seeking any legal remedy for a **Wrongful Act**.

### Damages

Damages that an **Insured** is legally liable to pay resulting from a **Claim** as ascertained by:

- (i) judgments or arbitral awards rendered against that **Insured**;
- (ii) monies payable by that **Insured** pursuant to any settlement agreement negotiated by that **Insured** and which is approved by the **Insurer**.

**Damages** includes punitive or exemplary or multiple damages where lawfully insurable.

### Defence Costs

Reasonable and necessary fees, costs and expenses which an **Insured** incurs with the prior written consent of the **Insurer**, in relation to the investigation, response, defence, appeal or settlement of a **Claim**, including court attendance costs incurred by or on behalf of that **Insured**.

**Defence Costs** does not include the remuneration of any **Insured**, cost of their time or any other costs or overheads of any **Insured**.

### Digital Media Activities

The posting on the **Company's** website or social media outlets, of any **Digital Media**.

### Digital Media

Any digitised content, including text, graphics, audio and video, that can be transmitted over the internet or computer networks.

### Insured

- (iv) A **Company**;
- (v) a natural person who was, is or during the **Policy Period** becomes a principal, partner, director, officer or **Employee** of a **Company**;

- (vi) an independent contractor, temporary contract labourer, self-employed person or labour-only sub-contractor, under the direction and direct supervision of a **Company**, but only in relation to the **Digital Media Activities** they undertake for that **Company**;
- (vii) a joint venture where a **Company** maintains operational control, but only to the extent of the **Company's** interest in such joint venture; and
- (viii) a natural person or entity which a **Company** is required by contract to add as an **Insured** under this policy, but only when and to the extent such natural person is acting on behalf of that **Company**;

provided that such organisation or person shall only be covered under this **Digital Media Content Liability Coverage Section** in respect of **Loss** arising from a **Wrongful Act** when undertaking **Digital Media Activities** in the foregoing capacities.

**Insured** includes the estate, heirs or legal representatives of a deceased, legally incompetent or bankrupt **Insured** referred to in (ii) above to the extent that a **Claim** is brought against them solely by reason of them having an interest in property that is sought to be recovered in a **Claim** against such **Insured** referred to in (ii) above.

### **Intellectual Property**

Copyright, trade mark, service mark, design rights, know-how, database rights, registered domain or any other intellectual property, but not including patents or trade secrets.

### **Loss Damages and Defence Costs;**

**Loss** does not include:

- (i) non-compensatory or multiple damages (except to the extent covered as **Damages**) or liquidated damages;
- (ii) fines or penalties;
- (iii) the costs and expenses of complying with any order for, grant of or agreement to provide injunctive or other non-monetary relief;
- (iv) discounts, service credits, rebates, price reductions, coupons, prizes, awards or other contractual or non-contractual incentives, promotions or inducements offered to an **Insured's** customers or clients;
- (v) production costs or the cost of recall, reproduction, reprinting, return or correction of **Digital Media** by any person or entity; or
- (vi) any **Insured's** remuneration, cost of time or overheads.

### **Wrongful Act**

Any actual or alleged:

- (i) defamation, including libel, slander, or disparagement of trade reputation or the character of any person or organisation, 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, domain name or license agreement;
- (iii) plagiarism, piracy or misappropriation or theft of ideas or information;
- (iv) invasion, infringement or interference with rights of privacy, publicity, morals, false light, public disclosure of private facts, intrusion and commercial appropriation of name, persona or likeness; or
- (v) passing-off but only if alleged in conjunction with any of the acts listed in (i) – (iv) above,

on or after the **Continuity Date** and prior to the end of the **Policy Period** in the course of undertaking **Digital Media Activities**.

## Exclusions

---

The following Exclusions are specific to this **Digital Media Content Liability Coverage Section**. They apply in addition to the Exclusions in Section 11 (Exclusions) of the **General Terms and Conditions**.

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

### **Anti –Trust**

Any actual or alleged antitrust violation, restraint of trade, unfair competition or unfair or deceptive business practices, including violation of any consumer protection law.

### **Assumed Liability, Guarantee, Warranty**

Any:

- (i) guarantee or express warranty made by an **Insured**; or
- (ii) contractual liability or other obligation assumed or accepted by an **Insured**.

### **Bodily Injury and Property Damage**

Any:

- (i) physical injury, mental illness, sickness, disease or death; or
- (ii) damage to or loss of or destruction of tangible property or loss of use thereof,

### **Employment Practices Liability**

Any of a **Company's** employment practices (including wrongful dismissal, discharge or termination, discrimination, harassment, retaliation or other employment-related claim).

### **Financial Data**

Errors made in any financial data that the **Company** publicises including the **Company's** annual report and accounts and any communications to the stock market.

### **Goods, Products or Services**

Any:

- (i) false advertising or misrepresentation in advertising of a **Company's** products or services;
- (ii) any failure of goods, products or services to conform with an advertised quality or performance; or
- (iii) infringement of trade marks or trade dress by any goods, products or services displayed or contained in any **Digital Media**.

### **Government/Regulatory Action**

Any

- (i) government, regulatory, licensing or commission action or investigation; or

- (ii) **Claim** brought by or on behalf of:
- a. ASCAP, SESAC, BMI, RIAA or any other music licensing organisation;
  - b. the Federal Trade Commission;
  - c. the Department of Health and Human Services or Office of Civil Rights;
  - d. the Federal Communications Commission; or
  - e. any other government, agency or office.

### **Infrastructure**

Any:

- (i) mechanical failure;
- (ii) electrical failure, including any electrical power interruption, surge, brownout or blackout; or
- (iii) telecommunications failure.

### **Insured v Insured**

Any **Claim** brought by or on behalf of an **Insured** against another **Insured** except a **Claim** by an **Insured** which directly results from another **Claim** by a **Third Party** first made during the **Policy Period** and covered by this **Digital Media Content Liability Coverage Section**.

### **Intentional Infringement of Intellectual Property**

Any intentional infringement of **Intellectual Property**.

### **Internal Messaging Services**

Any publication or broadcast of **Digital Media** posted or transmitted on any of the **Company's** internal instant message system, messaging boards, or chat rooms.

### **Over-Redemption**

Any price discounts, prizes, awards or other consideration given in excess of the total contracted or expected amount.

### **Ownership Rights**

Any **Claim** against the **Company** brought by or on behalf of any independent contractor, third-party distributor, licensee, sub-licensee, joint venture, venture partner, any employee of the foregoing, or any employee or agent of the **Company** arising out of, based upon or attributable to disputes over:

- (i) the ownership or exercise of rights in **Digital Media**; or,
- (ii) services supplied by such independent contractor, third-party distributor, licensee, sub-licensee, joint venturer, venture partner or employee or agent.

### **Patent/Trade Secret**

Any:

- (i) infringement of patents;
- (ii) loss of rights to secure registration of patents; or

- (iii) misappropriation of trade secrets.

#### **Royalties and other monies**

Any:

- (i) accounting or recovery of profits, royalties, fees or other monies claimed to be due from an **Insured**; or
- (ii) licensing fees or royalties ordered, directed or agreed to be paid by an **Insured** pursuant to a judgment, arbitration award, settlement agreement or similar order or agreement, for the continued use of a person or entity's copyright, trade mark, service mark, design rights, know-how, database rights, registered domain or any other intellectual property.

#### **Securities Claims**

Any:

- (i) actual or alleged violation by an **Insured** of any law, regulation or rule relating to the ownership, purchase, sale or offer of, or solicitation of an offer to purchase or sell, securities;
- (ii) any actual or alleged violation by an **Insured** of any provision of the Securities Act of 1933, the Securities Exchange Act of 1934 (each a United States of America statute) or any similar law of any jurisdiction; or
- (iii) any actual or alleged violation by an **Insured** of the Racketeer Influenced and Corrupt Organisation Act 18 USC Section 1961 et seq (a United States of America statute) and any amendments thereto or any Rule or Regulation promulgated thereunder.

#### **Trade Debts**

Any:

- (i) trading debt incurred by an **Insured**; or
- (ii) guarantee given by an **Insured** for a debt.

#### **Trading Losses/Monetary Value**

Any trading losses or trading liabilities, monetary value of any electronic fund transfers or transfers by or on behalf of an **Insured**.

#### **War and Terrorism**

Any war (whether war is declared or not), terrorism, invasion, use of military force, civil war, popular or military rising, rebellion or revolution, or any action taken to hinder or defend against any of these events.

## Territory Restriction Endorsement

In consideration of the premium charged, it is hereby understood and agreed that this policy is amended as follows: Notwithstanding anything to the contrary in this policy, or any appendix or endorsement added to this policy, there shall be no coverage afforded or benefit provided by this policy for any:

1. entity organized, headquartered, incorporated, registered or established in a **Specified Area**; or
2. natural person resident or located in a **Specified Area**; or
3. claim, action, suit or proceeding brought or maintained in a **Specified Area**; or
4. loss of, theft of, damage to, loss of use of, encryption of, interruption to the operations or availability of, or destruction of any property (tangible or intangible) located in a **Specified Area**, including, but not limited to, any computer system, data, money or securities located in a **Specified Area**.

For purposes of this endorsement, "Specified Area" means:

- a. The Republic of Belarus; or
- b. The Russian Federation as recognized by the United Nations (or their territories, including territorial waters, or protectorates where they have legal control; legal control shall mean where recognized by the United Nations).

Where there is any conflict between the terms of this endorsement and the terms of the policy, the terms of this endorsement shall apply, subject at all times to the application of any Sanctions clause.

If any provision of this endorsement is or at any time becomes to any extent invalid, illegal or unenforceable under any enactment or rule of law, such provision will, to that extent, be deemed not to form part of this endorsement but the validity, legality and enforceability of the remainder of this endorsement will not be affected.

**All other terms and conditions remain unchanged.**

## War and Terrorism Exclusion Amended Endorsement (23-03)

Applicable to such of the **Security and Privacy Liability Coverage Section**, the **Event Management Coverage Section**, the **Network Interruption Coverage Section** and the **Cyber Extortion Coverage Section** as are **Purchased**, the following endorsement is added to the policy.

It is hereby understood and agreed that:

1. Section 3, Exclusions, of each of the **Security and Privacy Liability Coverage Section**, the **Event Management Coverage Section**, the **Network Interruption Coverage Section** and the **Cyber Extortion Coverage Section** as are **Purchased** is amended by deleting the War and Terrorism exclusion.
2. Section 2, Definitions, of each of the **Security and Privacy Liability Coverage Section**, the **Event Management Coverage Section**, the **Network Interruption Coverage Section** and the **Cyber Extortion Coverage Section** as are **Purchased** is amended by deleting the definition of **Cyber Terrorism**.
3. The **Insurer** shall not be liable under the **Security and Privacy Liability Coverage Section**, the **Event Management Coverage Section**, the **Network Interruption Coverage Section** or the **Cyber Extortion Coverage Section** for any **Loss** arising out of, based upon or attributable to:

- (i) a **War**;
- (ii) a **Cyber Operation** that is carried out as part of a **War**; or
- (iii) a **Cyber Operation** causing an **Impacted State**,

provided, however, that (iii) immediately above shall not apply to a **Cyber Operation** on a **Computer System** used by an **Insured** or its third-party service providers that is not physically located in an **Impacted State**.

4. The following definitions apply solely to this endorsement. If there is an inconsistency between a definition set forth below and a definition for the same term in any other part of the policy, the definition below shall apply to the interpretation of this endorsement:

**Computer System** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.

**Cyber Operation** means the use of a **Computer System** by, at the direction, or under the control of a sovereign state to disrupt, deny access to, degrade, manipulate or destroy information in a **Computer System** of or in another sovereign state.

**Essential Services** means services that are essential for the maintenance of vital functions of a sovereign state including but not limited to financial institutions and associated financial market infrastructure, health services or utility services.

**Impacted State** means a sovereign state where a **Cyber Operation** has had a major detrimental impact on:

- (i) the functioning of that sovereign state due to critical disruption to the availability, integrity or delivery of an **Essential Services** in that sovereign state; or
- (ii) the security or defence of that sovereign state,

provided, however, that an **Impacted State** shall not result from an attack, or related series of attacks, solely impacting one or more **Insureds**.

**War** means armed conflict involving physical force either:

- (i) by a sovereign state against another sovereign state; or

(ii) as part of a civil war, rebellion, revolution, insurrection, military action or usurpation of power, regardless of whether war is declared.

**All other Terms, Conditions and Exclusions of this Policy remain unchanged.**



## Bricking Extension Endorsement

This endorsement amends the policy to the extent set out herein.

Applicable to **Event Management Coverage Section** only, it is understood and agreed that the schedule is amended to include the following:

|                         |           |            |                         |           |
|-------------------------|-----------|------------|-------------------------|-----------|
| <b>Event Management</b> | Purchased | Full Limit | As per policy retention | Inception |
| <b>Bricking</b>         | Purchased | Full Limit | As per policy retention | Inception |

It is further understood and agreed that Definition "Data Recovery Expenses" is deleted and replaced with the following:

### Data Recovery Expenses

The reasonable and necessary fees, costs and expenses incurred by a **Company** on actions taken to:

- (i) identify lost, damaged, destroyed or corrupted **Data**;
- (ii) determine whether any lost, damaged, destroyed or corrupted **Data** can be restored, repaired, recollected or recreated; and

restore, recreate, repair or recollect lost, damaged, destroyed or corrupted **Data** to substantially the form in which it existed immediately prior to the **Insured Event**, including where necessary the cost to restore **Data** from backups or the recreation of **Data** from physical records. Such costs may include the cost to replace any part of a **Company Computer System** on which such **Data** was stored that is no longer functional, but only where replacing such part is necessary to restore, recreate, repair or recollect such **Data** to mitigate the impact of an **Insured Event** and provided that the costs to replace such part of the **Company Computer System** is less than the costs to restore **Data** from backups or the recreation of such **Data** from physical records.

It is further understood that Exclusion 3.1 (Betterment) is deleted and replaced with the following:

### 3.1 Betterment

Consisting of the costs of:

- (i) updating, upgrading, enhancing, or replacing a **Company Computer System** to a level beyond that which existed prior to the occurrence of an **Insured Event**, however this Exclusion shall not apply to:
  - a. the patching or updating of a component of the **Company Computer System** required to resolve a **Security Failure** or **Breach of Confidential Information**; or
  - b. the replacement of a component of the **Company Computer System** required to restore, recreate, repair or recollect damaged, destroyed or corrupted **Data** which can only be reasonably replaced with an upgraded or enhanced component, but in such circumstances, only for the cost of such upgraded or enhanced component that most closely matches the functionality of the component to be replaced; or
- (ii) removing software program errors or vulnerabilities.

Applicable to **Event Management Coverage Section** and **Network Interruption Coverage Section** only, it is understood and agreed that the schedule is amended to include the following:

It is understood and agreed that Exclusion 3.2 (Bodily Injury and Property Damage) is deleted and replaced with the following:

### 3.2 Bodily Injury and Property Damage

Arising out of, based upon or attributable to any:

- (i) physical injury, mental illness, sickness, disease, or death; or
- (ii) loss, damage or destruction of tangible property; however this Exclusion 3.2 (ii) shall not apply to the loss of use of electronic equipment caused by the reprogramming of the software (including firmware) of such electronic equipment rendering it useless for its intended purpose.

**All other Terms, Conditions and Exclusions of the policy remain unchanged.**



## Reputational Harm

In consideration of the payment of additional **Premium**, or agreement to pay the additional **Premium**, the **Insurer** and the **Policyholder** agree that the **Event Management Coverage Section** is amended as follows:

The **General Terms and Conditions** are incorporated by reference into, made a part of, and are expressly applicable to this **Reputation Damage Endorsement**.

All cover under this **Reputation Damage Endorsement** is written on a primary basis and afforded solely with respect to **Insured Events** first discovered during the **Policy Period** and reported to the **Insurer** as required by the **General Terms and Conditions** and this **Reputation Damage Endorsement**.

The cover under this **Reputation Damage Endorsement** is subject to the **Limit of Liability** and to any other sub-limits stated in the **Schedule** and/or the **Endorsement Schedule**.

## Reputation Damage Endorsement Schedule

|                                 |            |
|---------------------------------|------------|
| Reputation Income Loss Sublimit | Full Limit |
| Maximum Period of Indemnity     |            |
| Waiting Period                  | 14 Days    |

### 1. Insurance Cover

---

The **Event Management Insurance Coverage 1.1** is amended to include the following:

(vii) **Reputation Damage;**

### 2. Definitions

---

The following definitions are specific to this **Reputation Damage Endorsement**. In the event that any of the below terms are already defined in the **Event Management Coverage Section** they shall have the meaning afforded below for the purposes of this **Reputation Damage Endorsement**. All other definitions set out within Section 4.2 - Definitions of General Applicability of the **General Terms and Conditions** and within Section 2 – Definitions of the **Network Interruption Coverage Section** shall apply as stated unless otherwise specified herein.

#### **Adverse Publicity**

The dissemination via any medium (including but not limited to dissemination via print, video, audio, electronic, or digital or digitized form) of previously non-public information specifically concerning an actual or alleged **Insured Event** affecting an **Insured's** customers or clients first discovered during the **Policy Period**. All **Adverse Publicity** relating to the same **Insured Event** shall be deemed to occur at the time of the first such **Adverse Publicity**.

#### **Income Loss**

The Net Income that would have earned by the Insured during the **Period of Indemnity** that is applicable to **Adverse Media** only

#### **Insured Event**

Any:

(ix) **Breach of Confidential Information**, or;

(x) **Security Failure**.

### Period of Indemnity

The period of time beginning at the time of the **Adverse Publicity** and elapsing after the **Maximum Period of Indemnity** specified in the **Reputation Damage Endorsement Schedule**.

### Reputation Damage

The **Company's Loss** as a result of **Adverse Publicity**.

The definition of **Loss** in Section 2 – Definitions of the **Event Management Coverage Section** is deleted in its entirety and replaced with the following:

### Loss

**Income Loss** sustained by the **Insured** during the **Period of Indemnity**.

## 3. Exclusions

---

The following exclusions are specific to this **Reputation Damage Endorsement** and shall not apply to coverage afforded under this **Policy** other than under this **Reputation Damage Endorsement**:

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

- (i) for the fees or expenses for the services of a public relations firm, crisis management firm or law firm to advise an **Insured** on minimizing the harm to an **Insured's** brand or reputation or restoring public confidence in an **Insured**.
- (ii) for public relations expenses, advertising expenses, or expenses to notify those persons or entities that may have been affected by the **Security Failure** or **Privacy Event**.
- (iii) arising out of, based upon or attributable to **Adverse Publicity** that refers or relates to the security or privacy of other entities in the same or similar business or industry as an **Insured**, including an **Insured's** competitors, unless there are specific assertions as to a **Security Failure or Privacy Event** affecting the **Insured**.
- (iv) for any liability to third parties regardless of reason, including, without limitation, any legal costs and expenses, liquidated damages, contractual penalties, civil or criminal fines or penalties, or consequential damages.
- (v) for any **Network Loss** covered under the **Network Interruption Coverage Section** (including as amended by endorsement).
- (vi) the impact of unfavourable business conditions.

## 4. Conditions

---

The following conditions are specific to this **Reputation Damage Endorsement** and shall apply in addition to the conditions set out within the **Event Management Coverage Section** and **General Terms and Conditions**.

### 4.1. Proof of Loss

In addition to the requirements to give notice to the **Insurer** under Section 2.1 – Notice and Reporting of the **General Terms and Conditions**, the **Company** must also:

- (i) complete and sign a written, detailed and signed proof of loss within one hundred and eighty (180) days of the date of their knowledge of the **Adverse Publicity**, which will include:
  - a. a full description of the **Loss** and the circumstances of such **Adverse Publicity**;

- b. a detailed calculation of any **Loss**; and

all underlying documents and materials that reasonably relate to or form a part of the basis of the proof of the **Loss**;

upon the **Insurer's** request promptly respond to requests for information. All

adjusted claims are due and payable forty-five (45) days after:

- a. the presentation of the satisfactory written proof of **Loss** as provided for in (a) and (b) above; and
- b. the subsequent written acceptance thereof by the **Insurer**.

The costs and expenses of establishing or proving **Income Loss** under this **Reputation Damage Endorsement**, including those associated with preparing the proof of loss, shall be the obligation of the **Company** and are not covered under this **Policy**. The **Insurer** will, however, meet the reasonable costs of the **Company's** auditors or external accountants in attending meetings and interviews and in providing such information as the **Insurer** shall request to verify and adjust the claim for **Income Loss**.

#### 4.2 Calculating Income Loss

When calculating **Income Loss** due consideration shall be given to the experience of the **Insured's** business before the **Adverse Publicity** and probable experience thereafter during the **Period of Indemnity** had no **Adverse Publicity** occurred and to the continuation of only those normal charges and expenses that would have existed had no **Adverse Publicity** occurred.

#### 4.3 Appraisal

If the **Company** and the **Insurer** disagree on the extent of **Income Loss**, either may make a written demand for an appraisal of such **Income 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 of this nature. Each appraiser will separately state the extent of **Income 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 costs, including the costs of their respective chosen appraiser, and (ii) bear the expenses of the expert equally.

**All other Terms, Conditions and Exclusions of the Policy remain unchanged.**

## I. General information

PLEASE COMPLETE EACH SECTION.

### Name & address of firm

|            |  |        |                            |
|------------|--|--------|----------------------------|
| Full name: | Oil & Gas Development Company Limited                    |        |                            |
| Address:   | Plot No 3,OGDCL Building, Jinnah Avenue F6/1, Blue Area, |        |                            |
| City:      | Islamabad  | State: | Fedral ZIP/postcode: 44000 |
| Website:   | www.ogdcl.com  |        |                            |

### Individual completing application form information

|            |                                 |  |  |
|------------|---------------------------------|--|--|
| Full name: | Kamran Yusuf Shami              |  |  |
| Title      | Chief Information Officer (CIO) |  |  |
| Email:     | kamran.shami@ogdcl.com          |  |  |

### Applicant's principal contact in the event of a security or privacy breach

|        |                                 |        |                        |
|--------|---------------------------------|--------|------------------------|
| Name:  | Kamran Yusuf Shami              | Email: | kamran.shami@ogdcl.com |
| Title: | Chief Information Officer (CIO) | Phone: | 03008540757            |

### Type of business

Sole proprietor  Corporation  Partnership  Other **Limited Company**

Date established: 20.09.1961

Business description: Exploration & Production (E&P)

## ANNUAL REVENUES

**Healthcare applicants:** Please provide net patient services revenues. All other applicants — please provide gross revenues.

|                       | Last complete financial year | Current year (estimate) | Next year (estimate) |
|-----------------------|------------------------------|-------------------------|----------------------|
| revenue               | USD 1,440 Million            | USD [ ]                 | USD [ ]              |
| International revenue | USD 0                        | USD [ ]                 | USD [ ]              |
| Gross profits         | USD 840 Million              | USD [ ]                 | USD [ ]              |

Do you generate revenues and have a presence i.e. “an establishment” in territories outside the U.S.?  Yes  No  N/A

If ‘Yes’, please provide a breakdown by appendix to this application. Please note that revenues in Canada and Australia should be further broken down by province and state for tax purposes.

Do you generate revenues and have a presence, i.e., “an establishment”, in territories Inside the EEA (excluding U.K.)?  Yes  No  N/A

If ‘Yes’, please list the territories:

### Approximate share of revenue attributable to:

Last complete financial year

[ ] % online trading

[ ] % business to business

[ ] % business to consumer

### Changes to the business:

Does the Applicant anticipate any changes in business activities, mergers, acquisitions, or operations during the next 12 months? If ‘Yes’, please describe in an appendix to this application.  Yes  No  N/A

Please describe any acquisitions, divestitures, and changes to business operations over the past 12 months.

[ ] No

Are newly acquired companies required to meet certain cybersecurity standards before they are connected to the network?  Yes  No  N/A

Is a cybersecurity audit part of the formal acquisition process?  Yes  No  N/A

## II. Risk assessment

### CYBERSECURITY GENERAL INFORMATION

Throughout this application, there are several important terms. For clarity, please use the following definitions to guide your answers.

- **Vital Assets:** Assets which are key to the organization's success and operation. **Vital assets** include, but are not limited to, applications which support business production, applications which store business critical and/or sensitive data, and core technology services such as directory services, document repositories, and email.
- **Domain Administrator:** User accounts, excluding **Service Accounts**, which are **privileged** (see below). In an Active Directory environment, this would include Enterprise Admins, Domain Admins, and the (built-in domain) Administrators groups, including nested groups/accounts. In Azure, this would include Global Administrators, Hybrid Identity Administrators, and **Privileged Role Administrators**.
- **Service Accounts:** Accounts used for running applications and other processes. They are not typically used by humans.
- **Privileged:** Any account having administrative rights in whatever solution is in use for directory services, identity provider (IdP), rights management, etc. In an Active Directory environment, this would include Enterprise Admins, Domain Admins, and the (built-in domain) Administrators groups, including nested groups/accounts. In Azure, this would include Global Administrators, Hybrid Identity Administrators, and **Privileged Role Administrators**.

1. Annual IT budget: **3million USD**

2. Budget spent on cyber security: **400 thousand USD**

3. Full-time IT employees: **25**

4. Full-time cybersecurity employees: **04**

5. How centralized is the Applicant's information security program? (Choose one)

a. Information security at the Applicant is centrally managed, and the policies apply to all operations. Where exceptions are made, it's by asset only (as opposed to by operation/legal entity).

b. Information security at the Applicant is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined below apply to greater than or equal to 98% of total endpoints.

c. Information security at the Applicant is centrally managed, but exceptions are made for certain operation/legal entities. The controls as outlined below apply to less than 98% of total endpoints.

d. Information security at the Applicant is federated, but the controls outlined below apply to greater than or equal to 98% of total endpoints.

e. Information security at the Applicant is federated, and the controls outlined below apply to greater than 50% of total endpoints, but less than 98% of total endpoints.

f. Information security is managed by individual legal entities or operating units. The controls below are based on a survey of all entities and operating units.

g. Don't know/other — Add addendum if other.

**Now moving towards managed SOC services including SIEM, SOAR & Threat Intelligence.**

6. Does the Applicant:

|  |            |    |     |            |
|--|------------|----|-----|------------|
| a. Have a Data Protection Officer or someone in charge of data security?   |            |    |     | <b>NO</b>  |
| b. Administer a corporate-wide policy governing security, privacy, and acceptable use of company property for all employees and independent contractors? | <b>Yes</b> | No | N/A |            |
| i. If 'Yes', does acceptable use policy include consequences for policy violations?  |            |    |     | <b>NO</b>  |
| ii. Are users disallowed from accessing social media platforms from organizational assets except where there is a defined business need?                 |            |    |     | <b>YES</b> |
| iii. Are users disallowed from accessing personal email from organizational assets?  |            |    |     | <b>NO</b>  |
| iv. Are administrators explicitly disallowed from internet use and personal email from their <b>privileged</b> accounts?                                 |            |    |     | <b>NO</b>  |
| v. Are users and administrators responsible for keeping their computers and accounts safe from common risks or issues?                                   |            |    |     | <b>YES</b> |
| vi. Are users and administrators required to report suspected violations?  |            |    |     | Yes        |
| c. Perform background checks on all employees and independent contractors with access to sensitive data?   |            |    |     | No         |
| d. Restrict user access to sensitive data/information based upon the job function of the employee or independent contractor?                             |            |    |     | Yes        |
| i. If 'Yes', is such access reconsidered on at least an annual basis?  |            |    |     | Yes        |

7. Does the Applicant use a third party or Managed Service Provider to administer their technology? **Yes**

a. If 'Yes', select all that are true: Applicant utilizes an MSP for:

|  |  |  |              |
|--|--|--|--------------|
| <b>Vital assets</b>                                      | <input checked="" type="checkbox"/> Security operations  | <input checked="" type="checkbox"/> Data backup and recovery | ERP          |
| <input checked="" type="checkbox"/> Cloud transformation | <input checked="" type="checkbox"/> Software development | Other (please describe)                                      | SAP Services |

b. If 'Yes', is the third party or Managed Service Provider given persistent access to the Applicant's resources, not needing authorization to connect? **No**

8. Does the Applicant have an inventory of all data stores, which includes the data owners, the asset it is stored on, sensitivity, retention limits and disposal requirements for at least all sensitive data? **Yes**

a. If 'Yes', is it updated at least annually? **Yes**

9. Has the Applicant defined and documented all **vital assets**? **Yes**

a. If 'Yes', is the vital asset inventory updated at least quarterly? **Yes**

10. Does the Applicant have a process to actively identify **vital assets**? **Yes**

11. Does the Applicant prioritize **vital assets** by importance to business operations? **Yes**

12. Does the Applicant have an inventory of all hardware assets, including end user devices, network devices, appliances, IoT devices, and servers? **Yes**

a. If 'Yes', does it contain: **Yes**

|                   |                  |              |             |
|-------------------|------------------|--------------|-------------|
| Static IP address | Hardware address | Machine name | Asset owner |
|-------------------|------------------|--------------|-------------|

b. What frequency is the inventory updated?

|          |               |           |   |
|----------|---------------|-----------|---|
| Annually | Semi-annually | Quarterly | Other ( <b>Daily basis specially for endpoints desktops/laptops</b> ) |
|----------|---------------|-----------|---|

13. Does the Applicant have a process to discover hardware assets on its network? **Yes**

a. If 'Yes', how frequently is process run? **Yes**

|              |       |        |         |                                    |
|--------------|-------|--------|---------|------------------------------------|
| Continuously | Daily | Weekly | Monthly | Other ( <b>Daily can be done</b> ) |
|--------------|-------|--------|---------|------------------------------------|

14. Does the Applicant have an inventory of all licensed software? **YES**

a. If 'Yes', what frequency is the inventory updated?

Annually    Semi-annually     Quarterly    Other

15. Does the Applicant have a process to decommission unused systems? **YES**

16. Does the Applicant use on-premises Microsoft Active Directory, regardless of whether it is authoritative?  
(We used azure AD) **NO**

17. Please state the number of servers operated by or on behalf of the Applicant:

18. Please state the number of endpoints operated by or on behalf of the Applicant:

Desktops: **2000**                      Laptops: **1000**                      Other (please specify):

19. Please state the percent of critical systems hosted:

On premises    **95%**    In a cloud environment    **5%**

If the Applicant has any further comments on questions in the section above, please elaborate below:

## DATA ASSESSMENT

1. Please identify nature of sensitive information stored by the Applicant:

| Sensitive information                         | Yes                                 | No                                  | N/A         | Records held (estimated) |
|---|-------------------------------------|-------------------------------------|-------------|--------------------------|
| a. Personally identifiable information        | <input checked="" type="checkbox"/> |                                     |             |                          |
| b. Medical records                            | <input checked="" type="checkbox"/> |                                     |             |                          |
| c. Financial information                      | <input checked="" type="checkbox"/> |                                     |             |                          |
| d. Driver license numbers                     |                                     | <input checked="" type="checkbox"/> |             |                          |
| e. Social Security/National Insurance numbers | <input checked="" type="checkbox"/> |                                     |             |                          |
| f. Other (please specify below)               |                                     |                                     | Employee ID |                          |

2. Please estimate the total number of unique individuals for whom records are currently stored by the Applicant. **11500**

3. In respect of 2., to the right, please estimate the maximum number of records held within a single database: **230000**

4. Does the Applicant process data for third-party companies? **Yes**

If 'Yes', please estimate the total number of records processed: **No**

If the Applicant has any further comments on questions in the section above, please elaborate below:

## EMPLOYEES

### Does the Applicant:

- |   |     |
|---|-----|
| 1. Require users to <u>change passwords on at least</u> a quarterly basis? (After 45 days)  | YES |
| 2. Require strong passwords for administrator rights, e.g., 10 characters using a mix of alphabetic, numeric, and other characters?                                     | YES |
| 3. Have a solution to prevent users from setting common and known-compromised passwords, even if they meet complexity requirements? (e.g. "1g2w3e4r5t" and "Passw0rd!") | NO  |
| 4. Enforce rotation of administrator access credentials at least every 30 days?   | NO  |
| 5. Require all employees and independent contractors to undergo annual cybersecurity training including phishing?   | NO  |
| 6. Terminate <u>user access rights</u> as part of its employee and independent <u>contractor exit</u> processes?  | YES |
| 7. Please confirm the total number of employees.  |     |
| 8. Please confirm the total number of computer users, if different than employee <i>count</i> . (3000 machines)   |     |
- If the Applicant has any further comments on questions in the section above, please elaborate below:

## MULTIFACTOR AUTHENTICATION

### Does the Applicant:

- |   |     |
|---|-----|
| 1. Require multifactor authentication for the following access?                             |     |
| a. Critical information inside the network  | YES |
| b. Remote network access  | Yes |
| i. <b>VPN</b> (MFA enabled for VPN)   | YES |
| ii. VDI   | Yes |
| iii. <b>Sensitive cloud applications</b>  | YES |
| iv. Sensitive web applications  | N/A |
| <b>c. Administrator and privileged accounts</b>   | YES |
| <b>d. Personal devices when connecting with the network</b>                                 | No  |
| <b>e. Independent contractors and vendors accessing the network</b>                         | No  |
| <b>f. Independent contractors and vendors accessing sensitive cloud or web applications</b> | No  |
| <b>g. Server access</b>   | No  |
| 2. Allow External Remote Desktop Protocol (RDP)? If 'Yes', are the following implemented:   | YES |
| a. VPN access only  | YES |
| b. Multifactor authentication for access  | YES |
| c. Network level authentication enabled   | YES |
| d. RDP honeypot(s)  | NO  |
| e. Other (Please identify)  | NO  |

3. Confirm the type(s) of MFA in place:

|                             |                  |                   |
|-----------------------------|------------------|-------------------|
| Push notification           | SMS/text message | Biometric         |
| ✓ Authenticator app         | Secondary email  | Certificate based |
| Token/physical security key | Other            |                   |

If the Applicant has any further comments on questions in the section above, please elaborate below:  
**(But MFA enabled only for Global Admins)**

**PRIVILEGED ACCESS MANAGEMENT**

**Does the Applicant:** *(Recently Purchasing PAM x NDR)*

1. Manage **privileged** accounts using tooling (e.g., CyberArk, PAM)? **NO**
2. Enroll any of the following accounts into a PAM tool? **NO**

| <b>Privileged</b> user accounts                    | <b>Service</b> accounts      |
|--|------------------------------|
| Domain administrator accounts                      | Local administrator accounts |
| Domain <b>service</b> accounts                     | Application accounts         |
| Backup accounts (used to manage or access backups) | Linux accounts               |

Other:

If 'No', please provide additional information for any local administrator accounts that are not enrolled into the PAM tool:

- a. Please confirm that identical local admin credentials are not used (i.e., there is not a common username and password used for each local admin accounts). Yes
- b. Please provide details below on how unauthorized local admin privilege escalation on workstation is detected: Using SIEM
- c. Have you implemented Microsoft's Local Administrator Password Solution (LAPS)? No

*(PAM Purchase in progress)*

3. Enabled the following features on the PAM tool:
- |  |     |
|--|-----|
| a. Credential time-out (please state time after which account locks):        | N/A |
| b. One-time passwords  | N/A |
| c. Credential rotation   | N/A |
| d. MFA   | N/A |
| e. Real-time monitoring of account activity/detection of suspicious activity | N/A |
4. How often are all **privileged** accounts (such as those used in Active Directory and SaaS solutions as well as Service and Local accounts) inventoried and reviewed? (If less than annually or not inventoried and refreshed, please provide explanation). Quarterly
5. Is logging and alerting configured for **privileged** account usage/changes? Yes
6. Are **domain administrator** accounts unique, separate accounts from other accounts used for everyday activities? Yes
7. Can **Domain Administrator** accounts can only be used from **Privileged** Access Workstations (which do not have access to internet or email)? No

8. Is there a log of all actions by **Domain Administrator** accounts for at least the past thirty days? **YES**

9. Please provide a count of the **Domain Administrator** accounts. 03

## LOCAL ADMINISTRATIVE & SERVICE ACCOUNTS

### Does the Applicant:

1. Prohibit workstations from local admin rights:

a. All of the time? **YES**

b. Case by case? **YES**

2. Have an inventory of all **privileged service accounts**? **YES**

If 'Yes', how frequently is it reviewed and updated?

(monthly)

3. Please provide number of **privileged service accounts**: (10)

a. For each **privileged** service account included above, please use the table provided in Supplement C of application.

4. Configure **service accounts** using the principle of least privilege? No

a. Are **service accounts** tiered such that different accounts are used to interact with workstations, servers, authentication servers, even for the same service? No

5. Configure **service accounts** to deny any interactive logon? No

If 'Yes', please confirm the percentage: %

6. Have specific monitoring rules in place for **service accounts** to alert for any abnormal behavior? No

7. Require service account passwords to be  $\geq 25$  characters? No

8. Require service account passwords to be rotated on a regular basis? No

If 'Yes', how frequently?

Annually    Semi-annually    Quarterly    Other

If the Applicant has any further comments on questions in the section above, please elaborate below:

## NETWORK OVERVIEW

### Does the Applicant:

1. Intrusion Detection Solution (IDS)? Product name: **NO**

2. Intrusion Prevention Solution (IPS)? Product name: (Fortinet 1000 D) **YES**

3. Endpoint Protection Platform (EPP)? Product name: (Microsoft defender) Yes

a. Does this include:    Endpoints/workstations    Servers

b. Do capabilities include isolation and containment? **YES**

c. Do capabilities include behavioral detection and exploit mitigation? **YES**

|  |            |
|--|------------|
| 4. Endpoint Detection and Response (EDR)? Product name: <i>(Microsoft defender)</i>  | <b>YES</b> |
| a. What % of Endpoints are protected by above? <i>(all)</i>  |            |
| b. What % of Servers are protected by above? <i>(all)</i>  |            |
| 5. Managed Detection and Response (MDR)? Product name: <i>(recently going to buy it)</i>   | <b>NO</b>  |
| 6. Network Detection and Response (NDR)? Product name: <i>(recently going to buy it)</i>   | <b>NO</b>  |
| 7. Security Information and Event Management (SIEM)? Product name: <i>(IBM.QRADAR)</i>   | <b>YES</b> |
| a. If using Active Directory, are domain controller logs ingested by the SIEM? <i>(yes)</i>  | <b>YES</b> |
| b. What information does the SIEM ingest?  |            |
| c. What percentage of Applicant's " <b>Vital Assets</b> " are ingested by SIEM   | 80%        |
| d. How long does SIEM retain logs? <i>03 months</i>  |            |
| 8. Data Loss Prevention solution (DLP) in place? Product name:   | <b>NO</b>  |
| a. Do alerts from the DLP feed into the SIEM?  | <b>NO</b>  |
| b. Is your DLP solution email or network based?  | <b>NO</b>  |
| c. Is your DLP solution in blocking mode?  | <b>NO</b>  |
| 9. Security Operations Center (SOC)? If 'Yes', <i>(case sent to press for managed SOC Services)</i>  | Yes        |
| a. 24x7 live coverage with eyes on glass?  | Yes        |
| b. Internally staffed?   | Yes        |
| c. Managed by a third party?   | <b>YES</b> |
| d. Does the SOC have authority and ability to remediate security events?   | No         |
| e. Is the SOC provided an updated list of <b>vital assets</b> at least quarterly?  | No         |
| f. Of the products referenced in questions 1-8 of this section, which are monitored by the SOC?  | Yes        |
| IPS    EPP    EDR    MDR    SIEM   |            |
| 10. Regarding the products referenced in questions 1-8 of this section, are all that require updated definitions done at least daily?            | No         |
| 11. Regarding the products referenced in questions 1-8 of this section, are all available anti-tamper features enabled?                          | No         |
| 12. Regarding the products referenced in questions 1-8 of this section, are all tools set to block suspected malicious activity vs. just notify? | No         |

|   |   |
|---|---|
| 13. If the Applicant is using Active Directory, which of the following Audit Policies are enabled on Domain Controllers? ( <i>Azure active directory in implementation phase</i> )  | Yes   |
| a. Audit Credential Validation (Failure)  | Yes   |
| b. Audit Process Creation (Success)   | Yes   |
| c. Audit Security Group Management (Success and Failure)  | Yes   |
| d. Audit User Account Management (Success and Failure)  | Yes   |
| e. Audit Other Account Management Events (Success and Failure)  | Yes   |
| f. Audit Sensitive Privilege Use (Success and Failure)  | Yes   |
| g. Audit Logon (Success and Failure)  | Yes   |
| h. Audit Special Logon (Success)  | Yes   |
| 14. Implement a hardened baseline configuration materially rolled out across servers, laptops, desktops, and managed mobile devices?  | <b>YES</b>  |
| 15. Employ vulnerability scanning across your enterprise?   | <b>NO</b>   |
| a. What % of the enterprise is covered?   | %   |
| b. What is the frequency of scanning?   | Constant    Daily    Weekly    Monthly    > Monthly <input checked="" type="checkbox"/> Quarterly |
| 16. Route all outbound web requests through a web proxy which monitors for and blocks potentially malicious content?  | <b>YES</b>  |
| 17. Implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft <a href="https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/learn-script-security">https://docs.microsoft.com/en-us/mem/configmgr/apps/deploy-use/learn-script-security</a> | <b>NO</b>   |
| 18. Segment your network based on certain criteria?   | <b>YES</b>  |
| The classification or level of information stored on your systems   | By geography  |
| System criticality  | Business function   |
| Subsidiaries  | Brick and mortar locations  |
| Other:  |   |
| 19. Segregate critical networks from internet facing or other less critical networks?   | <b>YES</b>  |
| 20. Do you segregate operational technology from information technology networks?   | <b>YES</b>  |
| 21. Configured host-based and network firewalls to disallow inbound connections by default?   | <b>YES</b>  |
| 22. An inventory of externally exposed assets?  | <b>YES</b>  |
| 23. Vulnerability scans of externally exposed assets?   | <b>YES</b>  |
| If 'Yes', what is the frequency? ( <i>quarterly</i> )   | Constant    Daily    Weekly    Monthly    > Monthly   |
| 24. Are Web Application Firewalls (WAF) in place for everything that is externally facing?  | <b>NO</b>   |
| a. If 'Yes', is the WAF in blocking mode?   | <b>NO</b>   |
| 25. Protective DNS service (e.g., Quad9, OpenDNS or the public sector PDNS)?  | <b>NO</b>   |
| 26. On externally exposed systems, disable or block those ports, services, and protocols known to allow the spread of ransomware? These include, but are not limited to <u>RDP</u> , SMBv1, SMBv2   | <b>(partially yes)</b>  |

|  |            |
|--|------------|
| 27. Penetration testing done by a third party?   | <b>YES</b> |
| a. If 'Yes', does the testing simulate known threat actor tactics, techniques, and procedures? | <b>YES</b> |
| If 'Yes', what is the frequency?   |            |
| Annually    Semi-annually <input checked="" type="checkbox"/> Quarterly    Other               |            |

If the Applicant has any further comments on questions in the section above, please elaborate below:

## EMAIL

### Does the Applicant:

|  |                             |
|--|-----------------------------|
| 1. Use any of the following email platforms?   |                             |
| <input checked="" type="checkbox"/> Microsoft Office 365   | Internal Microsoft Exchange |
| Google Workspace   | Other (please identify)     |
| 2. Enforce Multifactor Authentication (MFA) for all email accounts?  | <b>NO</b>                   |
| 3. Utilize an email monitoring/filtering solution (i.e. Microsoft ATP <i>(only for global admins)</i> , Proofpoint, Mimecast)? | <b>YES</b>                  |
| If 'Yes', enter solution.  |                             |
| 4. If 'Yes', does email monitoring/filtering solution perform any of the following?  |                             |
| a. Blocks known malicious links, attachments, and suspicious file types, including executables                                 | <b>YES</b>                  |
| b. Blocks suspicious messages based on their content or attributes of the sender   | <b>YES</b>                  |
| c. Has the capability to run suspicious attachments in a sandbox   | <b>YES</b>                  |
| 5. Use any of the following to protect against phishing messages?  | <b>YES</b>                  |
| SPF    DKIM and/or    DMARC  |                             |
| 6. Conduct regular phishing simulations of staff? If so, how often:  | <b>NO</b>                   |
| Monthly    Quarterly    Annually   |                             |
| 7. Measure-click through/fail rate?  | <b>NO</b>                   |
| a. Please confirm the rate   |                             |
| 0-5%    6-10%    11-16%    Higher fail rate  |                             |
| b. Is immediate additional training assigned for staff that fail phishing simulations?   | <b>NO</b>                   |
| 8. Is access to web-based email such as Outlook Web Access permitted?  | <b>YES</b>                  |
| If 'Yes', is MFA enforced  | Yes                         |
| 9. Allow access to web-based email such as Outlook Web Access?   | <b>YES</b>                  |
| 10. Filter/scan incoming emails for malicious attachments and/or links?  | <b>YES</b>                  |
| If 'Yes', do you have the ability to automatically quarantine, detonate, and evaluate attachments?                             | <b>YES</b>                  |
| 11. Disable macros in office productivity software by default? (e.g., Microsoft Office, Google Workspace)                      | <b>NO</b>                   |
| If 'Yes', are users allowed to enable macros?  | <b>YES</b>                  |
| 12. Disabled any of the following legacy email protocols?  |                             |
| Basic Authentication <input checked="" type="checkbox"/> IMAP <input checked="" type="checkbox"/> POP3    SMTP                 |                             |

If the Applicant has any further comments on questions in the section above, please elaborate below:

## PATCHING & SOFTWARE

- Documented no Policy but patch manager being used

### Does the Applicant:

1. Have a patching policy in place to install critical and high severity patches across the enterprise? If so, please **YES**

<24 hours  **24-72 hours** 2-7 days 7-30 days >30 days

a. Which systems are patched?

Internal servers  Workstations Perimeter systems

b. Is compliance with the policy tracked? **NO**

i. If 'Yes', what is the compliance rate?

>95% 90%-95% 80%-89% <80%

2. Have a patching policy in place to install normal severity patches across the enterprise? If so, please confirm **NO**

the time frame

24-72 hours 2-7 days 7-30 days >30 days

a. Which systems are patched?

Internal servers  Workstations Perimeter systems

Third Party Apps  Web browsers

3. Operate any end of life or end of support software or platforms? **NO**

a. If 'Yes', is it segregated from the rest of the network? N/A

b. If 'Yes', is sensitive PII data stored or processed on these assets? N/A

c. If 'Yes', do you purchase additional support for the software, where available? N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

## KNOWN VULNERABILITIES

1. Has the Applicant been affected by any known vulnerabilities rated 10 or above in the common vulnerabilities and exposures database (<https://nvd.nist.gov/general/nvd-dashboard/>)? (e.g. Keseya, Log4J, SolarWinds?) **NO**

a. If 'Yes', please outline any and all patching procedures, mitigating controls, investigations, or evidence of malicious activity below, or provide in an appendix

## BACKUPS & RECOVERY TIME

### Does the Applicant:

1. Conduct regular backup of data? **YES**

2. Frequently backup critical information? At least:

Continuously  **Daily**  **Weekly** Monthly Quarterly Semiannually Annually

3. Utilize physical backup tapes? **NO**

4. Store backups? Select all that apply:

Cloud  **On-premises**  Offline storage  **Off-site storage**  **Secondary data center**

5. If "Cloud" was selected in Question 4:

|   |    |
|---|----|
| a. Is your cloud-based backup service a "syncing service"? (e.g., DropBox, OneDrive, SharePoint, Google Drive)    | No |
| b. Have you determined how long it would take to restore all data from the cloud?                                 | No |
| c. Is access to cloud backups logged with alerts configured for suspicious activity?                              | No |
| d. Do you utilize versioning, data deletion prevention, and/or copies of the backups in other availability zones? | No |

6. If "Offline storage" was selected in Question 4, is this done at least:

Daily  Weekly  Monthly  Quarterly  Other (please identify)

7. If "Off-site storage" was selected in Question 4, is this done at least:

Daily  Weekly  Monthly  Quarterly

8. Subject backups to the following measures? Select all that apply

Multifactor authentication  Encryption  Segmentation  Virus/malware scanning  Immutable

If "Encryption" was selected in Question 8, is there an offline backup of encryption keys? No

9. Store unique backup credentials separately from other user credentials? Yes

10. Employ a physical and logical separation of backups from the rest of the network? Yes

If 'No', please outline the backup storage procedure:

11. Use unique accounts (not used for other systems) to access backups? Yes

12. Use accounts that are domain joined to access backups? No

13. Test a full recovery from a backup? If yes, the frequency of testing is at least: Yes

Daily  Weekly  Monthly  Quarterly  Other (please identify)

14. Test the integrity of backups prior to restoration to be confident it is free from malware? No

15. Maintain a warm or hot backup site for the purposes of resiliency, continuity, or redundancy? Yes

16. What is the Applicant's average time to triage and contain security incidents of workstations year to date?

>8 hours

If the Applicant has any further comments on questions in the section above, please elaborate below:

## NETWORK SECURITY ASSESSMENT

### Does the Applicant:

|  |     |
|--|-----|
| 1. Conduct security policy and procedure audits and remediate critical deficiencies?   | NO  |
| 2. Have physical security to control access to its data centers/server rooms? (e.g. 24 hr. guards, access cards, biometric access) | YES |
| 3. Replace factory default settings when configuring software and systems?   | YES |
| 4. Enforce a clear desk policy at all sites?   | NO  |
| 5. Have an enterprise-wide data retention and destruction policy?  | NO  |
| If 'Yes', is this policy regularly reviewed and updated?   | YES |
| 6. Have antivirus protection in place and is it updated frequently?  | YES |
| 7. Review antivirus software and firewalls, configurations, and settings on at least a quarterly basis?                            | YES |

8. Build information security measures into software that is developed or modified by internal resources? **No**

9. Require all connecting devices to have antivirus and firewall installed? **YES**

If the Applicant has any further comments on questions in the section above, please elaborate below:

## HANDLING & CRITICAL SENSITIVE INFORMATION (SENSITIVE INFORMATION AS DESCRIBED IN SECTION III.1. OF THIS APPLICATION)

### Does the Applicant:

1. Have data classification/categorization measures in place? **NO**

2. Isolate critical/sensitive information in its own segregated environment? **NO**

3. **Encrypt critical/sensitive information whilst at rest or in transit?** **Yes**

4. Use additional security measures such as tokenization or salting where applicable? **No**

If the Applicant has any further comments on questions in the section above, please elaborate below:

## MOBILE & PORTABLE DEVICES

### Does the Applicant:

1. Encrypt all sensitive data that is physically removed from your premises by laptop, mobile/portable devices, USB, backup tapes or other means? **NO**

If 'Yes', do you require storage on mobile and portable devices to be encrypted? **N/A**

**If 'No', please confirm whether you allow information to be downloaded onto portable devices.** **Yes**

2. Allow Bring-Your-Own-Device (BYOD) connections to the business network? (If only allowed to connect to guest Wi-Fi, choose "No") **NO**

If 'Yes', does the Applicant have a policy that governs BYOD usage and controls? **N/A**

3. Use a mobile device management system (MDM), which gives the ability to remote wipe the devices? **NO**

If 'Yes', is the MDM system applied to: Company-owned devices "BYOD" devices

4. Encrypt sensitive data when sent outside of its network (in transit)? **NO**

If the Applicant has any further comments on questions in the section above, please elaborate below:

## DATA RECOVERY & NETWORK BUSINESS INTERRUPTION ASSESSMENT

### Does the Applicant:

1. Have any of the following plans in place to address security or data breaches:

Incident response plan  **Business continuity plan**  **Disaster recovery plan**

a. If 'Yes', do the plan(s) clearly define the responsibilities and the support personnel for each key role? **YES**

b. If 'Yes', does the plan(s) include ransomware-specific response and recovery plans? **YES**

c. If 'Yes', are the plan(s) tested at least annually with any critical deficiencies remediated? **YES**

d. If 'Yes', are the plan(s) readily available in hardcopy? **YES**

|  |                   |                        |                         |                         |                    |
|--|-------------------|------------------------|-------------------------|-------------------------|--------------------|
| 2. Conduct cybersecurity incident tabletop exercises?  | <b>NO</b>         |                        |                         |                         |                    |
| a. Approximate date of last exercise?  | N/A               |                        |                         |                         |                    |
| b. Did the exercise include a threat from ransomware?  | N/A               |                        |                         |                         |                    |
| 3. Track how long it takes to restore the Applicant's <b>vital assets</b> following a network outage? If so, the length of time is:  |                   |                        |                         |                         |                    |
|  | Less than 8 hours | Between 8 and 12 hours | Between 12 and 24 hours | Between 24 and 72 hours | More than 72 hours |
| 4. Track how long it takes to restore the Applicant's non-critical systems following a network outage? If so, the length of time is: | Yes               | No                     | N/A                     |                         |                    |
|  | Less than 8 hours | Between 8 and 12 hours | Between 12 and 24 hours | Between 24 and 72 hours | More than 72 hours |
| 5. What is the Applicant's Recovery Time Objective (RTO)? (24 Hours)   |                   |                        |                         |                         |                    |
| a. Does the Applicant test and meet the RTO?   | <b>YES</b>        |                        |                         |                         |                    |
| If the Applicant has any further comments on questions in the section above, please elaborate below:                                 |                   |                        |                         |                         |                    |

## LEGAL & REGULATORY

### Does the Applicant:

|   |           |
|---|-----------|
| Have policies and procedures in place covering the following individuals' rights under countries' data protection regulations?  | <b>NO</b> |
| 1. Individuals are informed about the collection and use of their personal data   | <b>NO</b> |
| 2. Individuals have the right to access their personal data and a formal subject access request process is in place   | <b>NO</b> |
| 3. Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete, and a formal data rectification request process is in place | <b>NO</b> |
| 4. Individuals have the right to have personal data erased and a formal data erasure process is in place  | <b>NO</b> |
| 5. Individuals have the right to obtain and reuse their personal data for their own purposes across different services and a formal data portability policy is in place | <b>NO</b> |
| 6. Individuals have the right to object to the processing of their personal data and a formal objection policy is in place  | <b>NO</b> |
| 7. Have a lawful basis to carry out profiling and/or automated decision-making which is documented in our data protection policy  | <b>NO</b> |
| 8. Have a privacy policy?   | <b>NO</b> |
| If 'Yes'  |           |
| a. Is the privacy policy displayed on the Applicant's website?  | <b>NO</b> |
| b. Is the privacy policy approved by the Applicant's Board or legal department?   | <b>NO</b> |
| c. Is the privacy policy regularly reviewed and updated?  | <b>NO</b> |
| 9. Have a written, Board-approved policy that addresses compliance with applicable privacy and security laws or regulations?  | <b>NO</b> |

If you have answered 'No' to any of the questions above, please provide an explanation and information on your plans for compliance below.

If the Applicant has any further comments on questions in the section above, please elaborate below:

## VENDOR MANAGEMENT

1. Please identify all vendors that have access to or help to manage the Applicant's network or security systems:

| Name of vendor   | Nature of service                          | Does the vendor indemnify the Applicant under contract? |
|--|--|---|
|  | Data center hosting                        | YES   |
|  | Cloud services                             | YES   |
|  | Web hosting                                | YES   |
|  | Critical software                          | Yes   |
|  | Managed security services                  | YES   |
|  | Data processing services                   | No  |
|  | Endpoint detection and response            | NO  |
|  | Antivirus                                  | NO  |
|  | Firewall                                   | NO  |
|  | Intrusion detection and prevention systems | NO  |
|  | Internet service provider                  | Yes   |
|  | Data loss prevention                       | N/A   |
|  | Recovery services                          | NO  |
|  | Other (please state):                      | No  |
| 2. Are all vendors required to comply with the Applicant's security policy?  |  | YES   |
| 3. Are vendors audited to ensure that they meet the Applicant's security and privacy standards as well as those customary in the relevant industry and those mandated by regulators? |  | YES   |
| 4. Are vendor access rights periodically reviewed and updated?   |  | YES   |
| 5. Is vendor access on the Applicant's network monitored?  |  | YES   |
| 6. Is vendor access limited to dedicated time windows?   |  | NO  |
| 7. Does the Applicant periodically review all contracts to ensure that they satisfy data security and privacy laws and regulations?  |  | YES   |
| 8. Does the Applicant have a procedure to manage the termination of vendor contracts?  |  | YES   |
| 9. Does the Applicant require vendors to have cyber insurance coverage?  |  | NO  |

If the Applicant has any further comments on questions in the section above, please elaborate below:

## BIOMETRIC INFORMATION

### Does the Applicant:

1. Collect, store, process, use or retain any biometric information? If yes, please complete the following section. **YES**

2. Collect, receive, or retain any biometric data on employees or consumers as defined by law including (but not limited to):

Retina scan  Voiceprint  Iris scan  Hand scan  Fingerprint  **Face geometry** Other (please identify) [REDACTED]

3. Clearly define to employees, consumers, and/or individuals how the Applicant will:

Collect their biometric information  Use their biometric information  Destroy their biometric Information **NA**

4. Sell, lease, trade or otherwise profit from the biometric information of employees/consumers/individuals?    N/A

5. Subject biometric information to the following measures? Select all that apply.

Encryption in transit  Restricted access a least **privileged** basis  Encryption at rest

Segregated in an isolated environment  Other (please identify) **NA**

6. Obtain written consent from employees/consumers/individuals prior to collection, receipt, or retention of biometric data? **NO**

7. Have a retention schedule outlining how long biometric information is retained? **NO**

8. Have a data destruction policy for biometric information that is no longer required? **NO**

9. Has the Applicant received any complaints alleging the unlawful collection, use, dissemination, or sale of biometric data? If 'Yes', please describe: **NO**

If the Applicant has any further comments on questions in the section above, please elaborate below:

[REDACTED]

## PAYMENT CARD INDUSTRY ASSESSMENT

(complete only if applying for PCI DSS liability coverage)

### Does the Applicant:

1. Accept payment cards for its goods or services?  Yes  No  N/A

If 'Yes', is the Applicant compliant with PCI DSS Security Standards?  Yes  No  N/A

If 'No', please describe the current status of the Applicant's compliance work:

[REDACTED]

a. What Level of PCI Merchant is the Applicant? [REDACTED]

b. Approximately how many transactions were processed during the last 12 months? [REDACTED]

c. What is the approximate percentage of annual revenue attributable to credit card transactions? [REDACTED] %

2. Store payment card data on its network?  Yes  No  N/A

If 'Yes':

a. For how long is such data stored on the Applicant's network? [REDACTED]

b. Is payment card data either encrypted or tokenized at all times?  Yes  No  N/A

c. If the payment card data is not encrypted or tokenized, please describe what security protects such data in an appendix to this application.

[REDACTED]

3. Transact all payments through a payment processor?  Yes  No  N/A

If 'Yes':

a. Who is the payment processor? [REDACTED]

b. Has the payment processor provided evidence of its PCI DSS compliance to the Applicant?  Yes  No  N/A

4. Are 100% of your point to sale terminals EMV compliant?  Yes  No  N/A

If the Applicant has any further comments on questions in the section above, please elaborate below:

[REDACTED]

## MULTIMEDIA ASSESSMENT

(Complete only if applying for multimedia liability coverage)

### Does the Applicant:

1. Have a process in place to review media content (website, social media or otherwise) for the following prior to publication?

a. Infringement of copyright?  NO

b. Infringement of trademark  N/A

c. Libel or slander  N/A

d. Invasion of privacy?  N/A

2. Require a qualified attorney to review the above?  N/A

If 'No', please describe the procedures to avoid the posting of improper or infringing content:

[REDACTED]

3. Have a procedure for responding to any allegations which are in the nature of items 1. (i) to (iv) above?  NO

4. In respect of the Applicant's website:

a. Does the Applicant record visitor acceptance of terms of use before access is granted?  Yes  No  N/A

b. Does the website include third-party content?  Yes  No  N/A

If 'Yes':

i. Does this content include streaming video and music?  Yes  No  N/A

ii. Does the Applicant have procedures in place to secure rights for using all such third-party content?  Yes  No  N/A

|  |     |    |           |
|--|-----|----|-----------|
| c. Does the Applicant allow third parties to post content directly to the website?   |     |    | <b>NO</b> |
| d. Does the Applicant monitor content for offensive, harassing, infringing or other undesirable material?                      | Yes | No | N/A       |
| e. Does the Applicant reserve the right to remove or censor any content that violates the Applicant's acceptable terms of use? | Yes | No | N/A       |

If the Applicant has any further comments on questions in the section above, please elaborate below:

## Advertising activities

### 1. Marketing/advertising costs

|                | Past fiscal year | Current fiscal year | Next fiscal year |
|----------------|------------------|---------------------|------------------|
| U.S. costs     |                  |                     |                  |
| Non-U.S. costs |                  |                     |                  |
| Total costs    |                  |                     |                  |

### 2. Advertising channels: Please indicate the approximate percentages of advertising/marketing spending in each of the following channels:

|                    |   |                               |   |
|--------------------|---|-------------------------------|---|
| Television/cable   | % | Direct mail/catalog (print)   | % |
| Newspapers (print) | % | Digital/online (all channels) | % |
| Magazines (print)  | % | Other, please describe:       | % |

|  |     |    |     |
|--|-----|----|-----|
| 3. Have a procedure for responding to any allegations which are in the nature of items 1. (i) to (iv) above?   | Yes | No | N/A |
| 4. How many trade or service marks does the Applicant currently own?   |     |    |     |
| 5. For the proposed policy period, does the Applicant plan to use any of the Applicant's existing trade or service marks in connections with any new class(es) of goods or services for which the marks have not previously been used? | Yes | No | N/A |
| 6. Does the Applicant engage outside counsel specializing in trademark law in connections with the development or use of the Applicant's marks and products?   | Yes | No | N/A |
| 7. Does the Applicant always perform trademark clearance searches in connection with new marks or when expanding into new classes of goods or services?  | Yes | No | N/A |
| 8. Does the Applicant operate an in-house advertising agency? (i.e., does the Applicant create advertising and/or marketing content internally)?   | Yes | No | N/A |
| 9. Does the Applicant employ outside advertising agencies to create advertising or marketing content?  | Yes | No | N/A |
| 10. Does the Applicant utilize a website or social media to advertise or promote its products or services?   | Yes | No | N/A |
| 11. Does the Applicant have a written employee social media policy?  | Yes | No | N/A |
| 12. Does the Applicant have a process for legal review of all advertising, marketing, and promotional content, including website and social media content, prior to dissemination?   | Yes | No | N/A |
| 13. Has the Applicant ever received notification that any of its advertising, marketing or promotional content infringes on the intellectual property rights of others?  | Yes | No | N/A |

If the Applicant has any further comments on questions in the section above, please elaborate below:

## Media risk control & legal review

1. When providing technical, health-related or DIY related advice or guidance, does the Applicant always use a disclaimer or other warning?  Yes  No  N/A

2. Does the Applicant have formal, written policies and procedures for addressing requests to remove allegedly offensive or infringing content disseminated by or on behalf of Applicant?  Yes  No  N/A

3. Does the Applicant permit any User Generated Content ("UGC"), whether in the form of comments, videos, audio recordings, photographs/images, or other content, to be uploaded or shared on any of Applicant's websites or mobile apps?  Yes  No  N/A

4. Please indicate which of the following additional quality control/risk management procedures the Applicant uses in connection with the Applicant's media activities (select all that apply):

Website/social media content conduct and policy

Delay device used for live transmissions / broadcasts

Regular training of employees regarding libel and related claims

Regular training of employees regarding copyright, trademark, and other content claims

Other (please identify)

If the Applicant has any further comments on questions in the section above, please elaborate below:

## TECHNOLOGY E&O (INCLUDING MISCELLANEOUS PROFESSIONAL LIABILITY)

(complete only if applying for technology errors and omissions coverage)

1. Please provide a percentage breakdown of the Applicant's annual revenue between the following activities:

| Services and products  | Industries served    | Estimated % of revenue | Length of time sold or provided |
|--|----------------------|------------------------|---------------------------------|
| <b>Hardware</b>  |                      |                        |                                 |
| a. Sales of own brand  | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |
| b. Distribution of other brands                                      | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |
| c. Installation  | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |
| d. Maintenance   | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |
| <b>Software product sales</b>  |                      |                        |                                 |
| a. Sales of own brand shrink wrapped/off the shelf software          | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |
| b. Distribution of other brand shrink wrapped/off the shelf software | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |
| a. Customizable software   | <input type="text"/> | <input type="text"/>   | <input type="text"/>            |

| Services and products | Industries served | Estimated % of revenue | Length of time sold or provided |
|-----------------------|-------------------|------------------------|---------------------------------|
|-----------------------|-------------------|------------------------|---------------------------------|

**Software services**

- a. Installation, including configuration (no coding involved)
- b. Customization (including coding changes)
- c. Maintenance
- d. Systems integration
- e. End-user applications

**Services and products**

- a. Consultancy
- b. Contract staff
- c. Support services
- d. Project management
- e. Training
- f. Data management/ processing
- g. Data communication services
- h. Internet service provision of hosting

2. Please indicate the Applicant's five largest contacts/ projects:

| Client | Product/service | Contract revenues for this year/total contract value |
|--------|-----------------|--|
|        |                 |  |
|        |                 |  |
|        |                 |  |
|        |                 |  |

3. Does the Applicant provide professional services other those described above to customers or clients? Yes    No    N/A

If 'Yes', please describe:

a. What percentage of your revenues are derived from such professional services? %

4. What percentage of your work is performed by subcontractors? %

5. Operations controls

a. Does the Applicant have written contracts with all clients the Applicant performs work for or provides products to? Yes No N/A

If 'No', what percentage (%) of the time are they used? %

b. Do all services contracts with customers fully describe the scope of services to be provided? Yes No N/A

c. Do all contracts include how any disputes between the Applicant and the customer will be handled? Yes No N/A

d. Do all services and products contracts include provisions for the following:

i. Damages caps: Yes No N/A

If 'Yes', what is the standard cap on damages?

ii. Disclaimer of implied warranties Yes No N/A

iii. Guarantees Yes No N/A

iv. Full disclaimer of consequential damages Yes No N/A

If the response to Question 3.d.iv. is 'No', please explain the circumstances when a full disclaimer of consequential damages is not provided:

**Contractual procedures & controls**

1. Does the Applicant require the use of written contracts for all engagements? Yes No N/A

2. What is the average length and value of the Applicant's contracts?

3. Does the Applicant have a contractual review process? Yes No N/A

4. Please indicate the percentage of contracts used that are:

Applicant's standard contract: % Customers' contracts: % Customized or combination: %

5. Which of the following contractual provisions does Applicant always strive to impose in its favor in written contract (select all that apply)?

Disclaimer of warranties Indemnification/hold harmless

Alternative dispute resolution Limitation of liability

Exclusion of consequential damages Performance milestones

Exclusive remedies for breach Statement of work (SOW)

Force majeure Choice of law or venue

6. Does the Applicant have a formal customer acceptance of work/project completion process? Yes No N/A

7. Are performance milestones required to be accepted with signoff/approval by both parties? Yes No N/A

8. Are interim changes to SOWs or contracts documented and approved by both parties? Yes No N/A

9. Please describe the person by title or position employed by Applicant who have authority to alter or amend Applicant's standard contract language:

10. How many open/ongoing customer complaints/disputes is the Applicant currently handling?

## Quality control/risk management procedures

|   |  |
|---|--|
| 1. Does the Applicant employ a Risk Manager?  | Yes  |
| If you answered 'No' above, who is responsible for handling insurance-related matters?              |  |
| 2. Does the Applicant have written policies and procedures for responding to customer complaints?   | NA   |
| 3. Does the Applicant have an escalation procedure to respond to customer complaints?               | N/A  |
| 4. Which of the following quality control procedures does Applicant employ (select all that apply)? | NA   |
| Alpha testing   | Customer support by email or text                |
| Beta testing  | Formalized training for new employees            |
| Business continuity plan  | Prototyping with testing                         |
| Customer screening process  | Vendor certification and management procedures   |
| Customer support by telephone   | Written quality control standards and procedures |
| Customer support by web portal  | Other (please describe below):                   |

## CYBER CRIME/SOCIAL ENGINEERING

(complete only if applying for cyber/social engineering coverage) **NA**

### Does the Applicant:

|   |     |    |     |
|---|-----|----|-----|
| 1. Make payments to third parties by wire transfers?  | Yes | No | N/A |
| If 'Yes':   |     |    |     |
| a. How many times per week?   |     |    |     |
| b. What is the most common amount transferred?  |     |    |     |
| c. Do payments or transfers of a certain amount require dual authorization?   | Yes | No | N/A |
| 2. Have procedures in place to verify the receipt of goods or services against an invoice prior to payment?   | Yes | No | N/A |
| 3. Call a vendor using known prior telephone number to confirm any changes in bank account info, invoice amounts, location, contact number, fax number, etc.? | Yes | No | N/A |
| 4. Accept payments or funds transfer instructions from a customer or client relating to a refund or repayment of goods or services?                           | Yes | No | N/A |
| If 'Yes', what methods of receiving instructions are deemed acceptable (e.g. phone call, email, text message)?  |     |    |     |
| 5. Confirm all payments or funds transfers from a customer or client by a direct call to the customer or client using a previously known telephone number?    | Yes | No | N/A |
| 6. Have procedures in place to verify the authenticity of any payment request made by an internal company source (another employee, etc.)?                    | Yes | No | N/A |
| 7. Had any social engineering losses? If 'Yes', please describe.  | Yes | No | N/A |

### III. Claims & insurance history

#### CLAIMS

In the last five (5) years has the Applicant received or sustained, or are there currently pending, any claims, complaints or incidents which may be covered under the proposed insurance and/or does the Applicant have knowledge of any fact, circumstance, situation, event, or transaction which may give rise to a claim or loss under the proposed insurance?

NA

If 'Yes', please provide details in an appendix to this application.

#### INSURANCE HISTORY

1. During the last five (5) years, has any insurance policy providing substantially the same or similar insurance as the insurance being applied for under this application been declined, canceled or nonrenewed at the choice of the insurer?

No

2. Does the Applicant currently have insurance in place covering privacy or data security exposures?  
If 'Yes', please confirm:

No

| Insurer | Aggregate policy limit | Self-insured retention | Inception date | Expiry date | Retroactive date | Premium |
|---------|------------------------|------------------------|----------------|-------------|------------------|---------|
|         |                        |                        |                |             |                  |         |
|         |                        |                        |                |             |                  |         |

## IV. Declaration

The undersigned authorized representative of the Applicant declares that the statements set forth herein are true. The signing of this application does not bind the undersigned or the insurer to complete the insurance. It is represented that the statements contained in this application and the materials submitted herewith are the basis of the contract should a policy be issued and have been relied upon by the insurer in issuing any policy. The insurer is authorized to make any investigation and inquiry in connection with this application as is reasonable and necessary. Nothing contained herein or incorporated herein by reference shall constitute notice of a claim or potential claim so as to trigger coverage under any contract of insurance.

This application and materials submitted with it shall be retained on file with the insurer and shall be deemed attached to and become part of the policy if issued. It is agreed in the event there is any material change in the answers to the questions contained in this application prior to the effective date of the policy, the Applicant will notify the Insurer in writing and any outstanding quotations may be modified or withdrawn at the insurer's discretion.

Must be signed by a corporate officer with authority to sign on the Applicant's behalf.

Signed:

Kamran Yusuf Shami

Title:

Chief Information Officer (CIO)

Print name:

Kamran Yusuf Shami

Date:

1/12/2025

# Supplementary questions

## SUPPLEMENT A — HEALTHCARE ASSESSMENT

1. Is the Applicant compliant with HIPAA?  No
2. When was the Applicant's compliance with HIPAA last reviewed?
3. Does the Applicant host or use a healthcare exchange to share data with other healthcare organizations?  Yes  No  N/A
- If 'Yes', please describe what data is being shared and with whom:

## SUPPLEMENT B — OPERATIONAL TECHNOLOGY (E.G., SCADA, DCS, CIM, CNC, ETC.)

1. Please provide an overview of the Operational Technology (OT) on your network:
- (all – OT devices are isolated from network)*
2. Please provide an overview of the team responsible for OT and their reporting structure:
- Production Directorate/Exploration Directorate
3. Do you employ a dedicated OT cyber security professional? **NO**
4. Do you maintain an up-to-date inventory of all IT and OT assets identifying 100% of your assets?   No
- a. If not 100% please estimate the percentage of OT assets inventoried as well as any compensating controls for non-inventoried assets  %
5. What is the highest dependency you have on any one facility? No
6. What percentage of maximum capacity is your production facility running? 30  %
7. In the event of an outage, can you make up the lost production at the facility affected by adding shifts or running at a higher capacity at this or another facility?   No
8. How many days of finished inventory do you hold at your production facility or distribution warehouse? NA
9. Does the Applicant utilize the following technologies to physically or logically segregate your IT and OT networks?
- Air Gap    DMZ    Firewall    VLAN
- If VLAN is selected, please describe the degree to which traffic is restricted and what technical control is used to enforce segmentation.
- 
10. Is MFA required for remote access to OT environment? **NO**
- a. If 'No', describe any additional security in place
-

11. Are the following in place to further secure your OT environment? (**No -OT infra is totally air gaped**)

|  |  |
|--|--|
| <input type="checkbox"/> Application whitelisting    | <input type="checkbox"/> Disabled removable devices      |
| <input type="checkbox"/> Managed security patching   | <input type="checkbox"/> Intrusion detection systems     |
| <input type="checkbox"/> Intrusion prevention system | <input type="checkbox"/> SIEM                            |
| <input type="checkbox"/> Endpoint protection         | <input type="checkbox"/> Third-party penetration testing |

12. Have all default usernames and passwords in the OT environment been removed/modified? **NO**

13. Do you allow remote access to OT environment?

If 'Yes', what security is in place:

[Redacted]

14. Is the use of removable devices (e.g., USB memory sticks) disabled within the OT environment? **NO**

If 'No', what security is in place:

[Redacted]

15. Do all OT assets using legacy software (e.g., Windows XP) have enhanced security? **NO**

a. Why are these systems still in place?

[Redacted]

b. Are there any compensating controls in place to mitigate the risk? **NO**

[Redacted]

c. What plans exist to upgrade or remove these systems? **NO**

[Redacted]

16. Do you prevent browsing the Internet and checking email on industrial systems? **NO**

17. Is OT restoration explicitly addressed in your disaster recovery plan? **NO**

18. Are your OT environments included in your backup strategy? **NO**

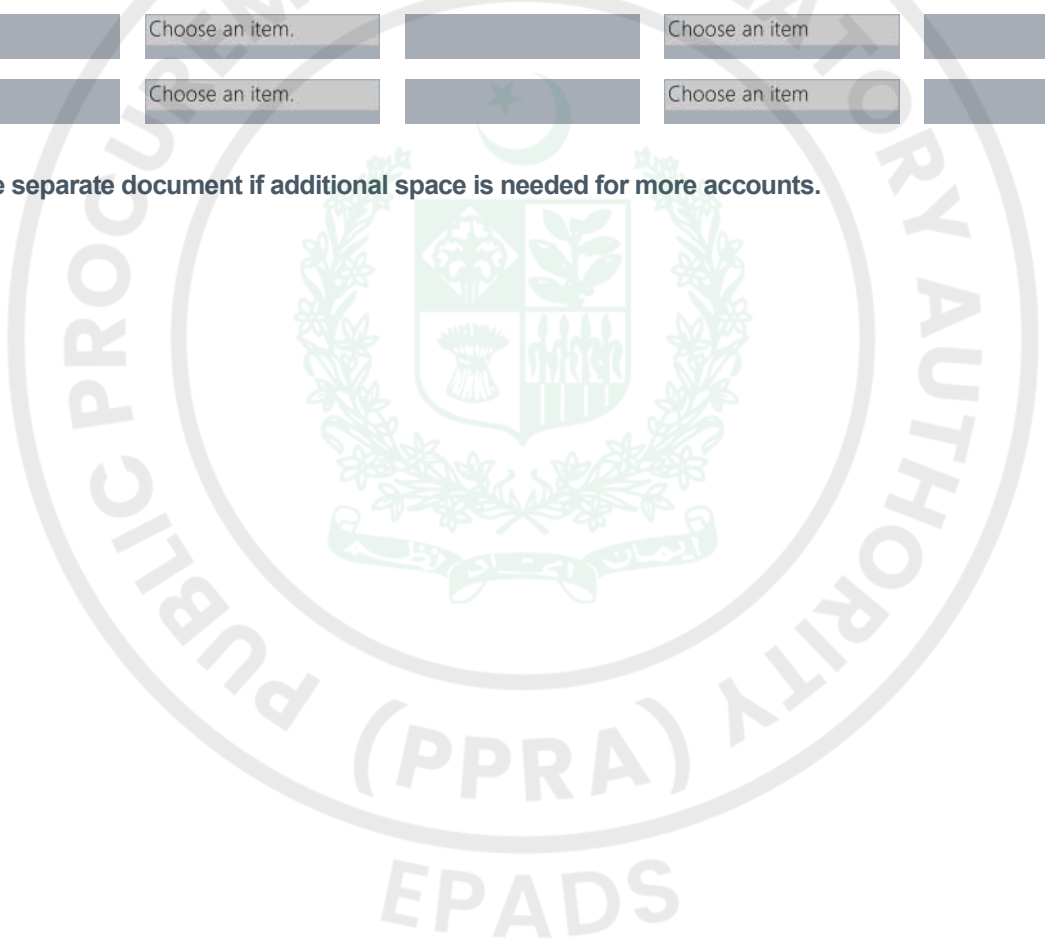
Please describe any difference between how they are stored and other backups

[Redacted]

**SUPPLEMENT C — PRIVILEGED SERVICE ACCOUNT APPENDIX**

| Name of account | Privileges it has | Software product it supports | What hosts it authenticates to | Why are the privileges required |
|-----------------|-------------------|------------------------------|--------------------------------|---------------------------------|
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |
|                 | Choose an item.   |                              | Choose an item                 |                                 |

**Please use separate document if additional space is needed for more accounts.**



**“Broker’s Letter Head”**

**Subject:** Oil and Gas development Company Limited  
 Cyber Reinsurance  
 Period from:12 months (to be advised)  
 Method of tender: Single Stage-Two Envelope Basis  
**Technical Compliance Matrix sheet**

| <b>Tender Requirement</b>   | <b>Means of Verification</b>  | <b>Compliance (Yes/No)</b> |
|---|---|----------------------------|
| Foreign brokers as well as local affiliates to submit valid professional indemnity policies meeting regulatory requirements of their respective countries of registration.              | Indemnity Policy  |                            |
| Name of Lead Reinsurer  | Broker’s Letterhead<br>duly Signed &<br>Stamped                     |                            |
| Lead Reinsurer Rating: minimum “A” as per S&P/AM Best Moody’s and Fitch   |   |                            |
| Lead Reinsurer Share: at least 15% not more than 25%  |   |                            |
| Country of Origin:  |   |                            |
| Quotation should be “FIRM” quote  | Signed & Stamped<br>Slip & Affirmation<br>on Broker’s<br>Letterhead |                            |
| Validity of quote should be 45 days from date of opening of bid   |   |                            |
| No underwriting agencies are allowed as leader  |   |                            |
| Quotation/slip/policy wording should be without any expressed or implied subjectivities/conditions/additional exclusions/warranties   |   |                            |
| Premium Payment warranty should be ninety (90) days from the inception of the policy period   |   |                            |
| Law and Jurisdiction must be (Pakistan)   |   |                            |
| Actual Quotation slip/policy wording signed/stamped by the leader must be attached  |   |                            |
| <b><u>Limit of Liability</u></b>  |   |                            |
| USD 10,000,000 each and every claim and in the aggregate including costs and expenses   |   |                            |
| The overall Aggregate limit of indemnity for all Insuring Clauses is USD 10,000,000   |   |                            |
| <b><u>Deductibles</u></b>   |   |                            |
| <ul style="list-style-type: none"> <li>• USD 250,000 each and every claim</li> <li>• Network Interruption Loss Waiting Hours: 12 Hours</li> <li>• Reputational Harm: 14 Days</li> </ul> |   |                            |

Name of Broker: \_\_\_\_\_

Signature: \_\_\_\_\_

Stamped: \_\_\_\_\_

Dated: \_\_\_\_\_

## Broker's Letter Head

**Subject:** Oil and Gas development Company Limited  
Cyber Reinsurance  
Period from: 12 months (to be advised)  
Method of tender: Single Stage-Two Envelope Basis  
**Financial Compliance Matrix sheet**

| <b>Particulars</b>                                      | <b><u>Amount in USD</u></b> |
|---|-----------------------------|
| Gross Premium (100%) including all layers (if any)      |                             |
| Less: Client Discount (if any non-conditional discount) |                             |
| Premium after Discount                                  |                             |
| Add: Broker Fee (if applicable)                         |                             |
| <b>Premium 100% (payable by client)</b>                 |                             |
| Less: Reinsurance Commission                            | <b>10%</b>                  |
| Net to Broker 100%:                                     |                             |

Name of Broker: \_\_\_\_\_

Signature: \_\_\_\_\_

Stamped: \_\_\_\_\_

Dated: \_\_\_\_\_