



**Assurance**

Covers You Right Through

## **Proposal Form Cyber Liability Insurance**

(The liability of the Company does not commence until this proposal has been accepted by the Company and the premium paid.)

1. Information given herein will be treated in strict Confidence.
2. Put a (✓) mark wherever applicable.
3. If space is not sufficient in any column, please give details on a separate sheet of paper.
4. Kindly answer all questions completely in order to help us to serve you better.

### **Important Notice**

This is a proposal form for a Claims Made policy. The policy will only respond to claims and/or circumstances which are first made known to the Insured and notified to Liberty Assurance Limited during the policy period.

The policy will not provide cover for:

- Events that occurred prior to the retroactive date of the policy (if specified).
- Claims made after the expiry of the policy period (or extended reporting period if available) even though the act giving rise to the claim may have occurred during the policy period.
- Claims notified or arising out of facts or circumstances notified under any previous policy or noted on the current proposal form or any previous proposal form.
- Claims made, threatened or intimated prior to the commencement of the policy period.
- Claims arising from circumstances known to the Insured at the commencement of the policy period as having the potential to give rise to a claim.

### **A. Applicant Details**

Name of Applicant	
Trading Name / Subsidiaries	
Any Other Party to be Insured; please give details including relationship with the applicant	
Address	
Website	
Email	
Contact Person	
Phone	
Mobile	



**Assurance**

Covers You Right Through

Broker / Agent	
Nature of Business	

### Turnover/Revenue and General Information

Country	Turnover (PGK)	Revenue created online (PGK)

### IT Budget & Security Spend

What is your IT budget?	
What percentage of your budget is allocated to IT security	

### Quality and Quantity of Data, Online Activities & Services

<b>What type of sensitive data is your Company maintaining / processing?</b>	
<input type="radio"/> Personally Identifiable Information (PII)	<input type="radio"/> The Payment Card Industry Data Security Standard (PCI DSS)
<input type="radio"/> Personal Health Information (PHI )	<input type="radio"/> Intellectual Property (IP)
<input type="radio"/> Usernames and Passwords	

### Please state the (estimated) volume of sensitive data (number of unique records) your Company maintaining/ processing

1,000       1,000-10,000       10,000-100,000       100,000+

### Please state the (estimated) number of user endpoints (desktops, laptops, portable media)

< 25       11-50       51-100       100 +

### B. (i) Cover Required

<b>Limit of Indemnity</b>	<input type="checkbox"/> 250,000	<input type="checkbox"/> 500,000	<input type="checkbox"/> 1,000,000	<input type="checkbox"/> 2,000,000	<input type="checkbox"/> 5,000,000	<input type="checkbox"/> 10,000,000
<b>Business Interruption</b>	<input type="checkbox"/> 100,000	<input type="checkbox"/> 250,000	<input type="checkbox"/> 500,000	<input type="checkbox"/> 1,000,000	<input type="checkbox"/> Full Policy Limit	
<b>Systems Damage</b>	<input type="checkbox"/> 50,000	<input type="checkbox"/> 100,000	<input type="checkbox"/> 250,000	<input type="checkbox"/> 500,000	<input type="checkbox"/> 1,000,000	



**Assurance**

Covers You Right Through

<b>Cyber Crime</b>	<input type="checkbox"/> 100,000	<input type="checkbox"/> 250,000			
<b>Extortion</b>	<input type="checkbox"/> 50,000	<input type="checkbox"/> 100,000	<input type="checkbox"/> 250,000	<input type="checkbox"/> 500,000	<input type="checkbox"/> 1,000,000

### **B. (ii) Optional Extensions**

- Named Cloud Service Provider Yes  No  If Yes, please name Cloud Provider
- Fraudulent Impersonation Yes  No   
If Yes please answer the following questions
  - (a) Are all payments to suppliers done via an email platform or provider that uses anti-spoofing systems or allows multi-factor authentication? Yes  No
  - (b) Are digital signatures used for email exchanges with all suppliers? Yes  No
  - (c) Do you use a purchase order numbering system? Yes  No
  - (d) Are checks performed that goods or services were both ordered and delivered/received before paying an invoice? Yes  No
  - (e) Are all changes of bank account details of a partner or supplier validated by a channel other than email, ie. by telephone call to a trusted number? Yes  No   
 If Yes please provide details
  - (f) Are all staff handling payments trained to recognise suspicious emails?  
Yes  No

### **C. IT Controls (Answer Yes / No)**

Control	Yes	No
Dedicated IT security person/team	<input type="checkbox"/>	<input type="checkbox"/>
Regular staff security awareness training	<input type="checkbox"/>	<input type="checkbox"/>
Password policy enforced	<input type="checkbox"/>	<input type="checkbox"/>
Systems patched monthly	<input type="checkbox"/>	<input type="checkbox"/>
Incident response plan tested annually	<input type="checkbox"/>	<input type="checkbox"/>
Disaster recovery plan tested annually	<input type="checkbox"/>	<input type="checkbox"/>
Firewall in place	<input type="checkbox"/>	<input type="checkbox"/>
Anti-virus / malware protection	<input type="checkbox"/>	<input type="checkbox"/>
Off-site backups performed	<input type="checkbox"/>	<input type="checkbox"/>



**Assurance**  
Covers You Right Through

## **D. Third Party Services**

1. Do you outsource any part of your network, computer system or information security functions? Yes  No

2.  If Yes please give details

Function Provider

- Management of entire IT system
- Data Processing)
- Application of Service Provider
- Offsite Backup and Storage
- Other Cloud Computing Services

3. Do you have a written and signed contract with the respective service provider(s) including a non -disclosure / confidentiality agreement?

(N/A only if you do not outsource any part of your network, computer system or information security functions) Yes  No  N/A

## **E. IT Security**

1. Organisational Protection

a) Do you have a dedicated IT Security person or team who regularly reports to senior management? Yes  No

b) Are you required to be PCI (The Payment Card Industry Data Security Standard) compliant? Yes  No

c) Do you provide regular training to increase your staff's security awareness and to prepare employees to be more resilient and vigilant against phishing? Yes  No

d) Do you have a password policy and is it enforced e.g. by complexity (strong passwords) and rotation (regular change)? Yes  No

e) How often are passwords required to be changed?

f) Do you regularly – at least monthly – patch (update) your systems and applications? Yes  No

g) Do you immediately apply critical patches (updates) to your systems and applications? Yes  No



**Liberty Assurance**  
Covers You Right Through

h) Do you have an incident response plan and is it at least annually tested? Yes  No

i) Do you have a disaster recovery plan and is it at least annually tested? Yes  No

j) Do you restrict user access/privileges to a need -to-do-business only? Yes  No

k) Do you immediately remove access of terminated or temporary staff? Yes  No

l) Do you provide users remote access? Yes  No

i.  If Yes, is access granted via a Virtual Private Network (VPN) or equivalent?  
Yes  No

and

ii. Does access require two -factor authentication (ie not just username and password)? Yes  No

m) Do you have an information classification scheme (ie identify mission critical information assets)? Yes  No

If Yes, does the scheme take into account information confidentiality, integrity and availability? Yes  No

## 2. Technical Protection

a) Do you use anti-virus, anti-spyware or equivalent malware protection?  
 If Yes, are all malware protection software automatically updated? Yes  No

b) Are all internet access points to your network secured by firewall(s)? Yes  No

c) Is it ensured that all default passwords on all computer systems (e.g. router) are changed? Yes  No

d) Is all personally identifiable and confidential information encrypted when:  
i. At rest?  ii. In transit/motion? Yes  No

e) Do you perform regular, automatic off-site backups? Yes  No   
 If Yes, how often? At least daily  At least weekly

f) Do you test retrieval of backups? Yes  No

g) Do you have a business continuity plan and is it at least annually tested? Yes  No



**Liberty Assurance**  
Covers You Right Through

h) Do you run external vulnerability scans or undertake penetration testing against your network? Yes  No

#### **F.(a) Prior Insurance**

a) Do you currently hold, or have you ever held cyber insurance providing the same or similar coverage as the insurance sought? Yes  No

b) Has any insurer ever cancelled or non-renewed a policy that provided the same or similar coverage as the insurance being applied for? Yes  No

c) Required an increased premium or imposed special conditions? Yes  No

d) Declined an insurance claim by the Applicant or reduced its liability to pay an insurance claim in full (other than by application of an Excess)? Yes  No

If Yes to any of the above please give details

#### **F.(b) Claims & Loss History**

(a) Any cyber incidents or losses in last 3 years?  Yes  No

If Yes, provide details including financial details:

(b) Within the last 3 years have you notified your customers that their information was or could be compromised Yes  No

© Within the 3 years has a customer claimed that their personal data has been compromised? Yes  No

If Yes, what was the financial loss associated with it for your company?

(d) Past Claims - Has any claim been made against the Applicant or any principal or director (including principal or director of any previous business) consultant or employee in respect of the risks to which this proposal relates? Yes  No

(e) Has the Applicant or any principal, partner, director, consultant or employee incurred any other loss or expense which might be within the terms of this insurance Yes  No   
If Yes, please give details

(e) Potential Claims - Is any principal, director, partner consultant or employee, after enquiry, aware of any circumstances which might:

1. give rise to a claim against the Applicant or his/her predecessors in business or any



**Assurance**  
Covers You Right Through

present or former principals, partners, directors, consultants or employees? Yes  No

2. result in the Applicant or his/her predecessors in business or any present or former principals, partners, directors, consultants or employees incurring any losses or expenses which might be within the terms of this insurance cover (this includes but not limited to disciplinary hearings) Yes  No

If Yes, please give details

### **Declaration**

I/We declare that the information provided is true and correct and forms the basis of the insurance contract.

Name	
Title	
Signature	
Date	

### **IMPORTANT NOTE**

1. *Specimen copy of the Policy Form and other terms applicable to risk is available, on request by the Proposer.*
2. *Please note that the above is for your general information only. For further details and specific information, please refer to the Policy whose terms and conditions, exceptions, clauses and warranties are applicable to this insurance.*
3. *The Policy holder shall keep a record of all information including copies of letters supplied to the insurers for the purpose of entering into the contract. A copy of the completed Proposal Form will be supplied to the Proposer on request after its completion*