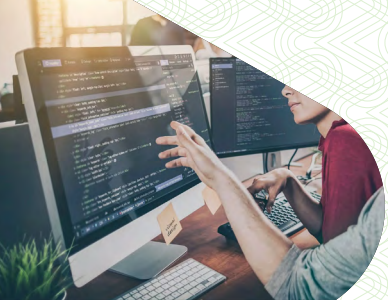

Cyber
Liability Insurance
Proposal form

delta

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 against you and notified to Delta Underwriting Private Limited during the policy period.

This proposal forms the basis of any insurance contract entered into. Please complete it fully and carefully remembering to sign the Declaration. If you have insufficient space to complete any of your answers, pleas continue on a separate attachment.

You have an ongoing duty to disclose all material facts and failure to do so could prejudice future claims.

ALL answers should be given as a group response i.e., if any subsidiary company has different responses (e.g. different controls and policies), these should be made known and provided separately to us.

COMPANY INFORMATION

1 Name of Insured:

2 Date Established:

3 Name of any other entity to be Insured (Please specify the corporate relationship with the Name Insured):

4 Website:

5 Principal address of Insured:

6 Business Description:

7 Geographical Split of Income:

Country	Last financial year (actual)	Current financial year (projected)
Singapore	$	$
Asia (specify)	$	$
Far East	$	$
New Zealand	$	$
Australia	$	$
UK / Europe	$	$
USA/Canada	$	$
Rest of world	$	$
Total	**$** 0	**$** 0

BUSINESS ACTIVITIES

8 Does the Company allow online; purchases, bill payments, banking or trading? ○ Yes ○ No

If Yes, what portion of the applicant's revenue is received through the online distribution channel? %

9 What types of personal information does the Company collect, process and store?

○ Business & Customer Information ○ Healthcare Information ○ Tax Numbers ○ Credit Card Information

○ Financial Account Information ○ Intellectual Property/Trade Secrets

10 If Credit Card is selected above, does the Company comply with Payment Card Industry Data Security Standards? ○ Yes ○ No

(a) Is the access to such sensitive data restricted? ○ Yes ○ No

(b) Who has access?

11 Does the Company use Industrial Control systems (ICS), such as Supervisory Control and Data Acquisition (SCADA), Distributed Control Systems (DCS), or Programmable Logic Controllers (PLC)? ○ Yes ○ No

12 Does the company maintain a public facing website? ○ Yes ○ No

If Yes, what applications, services or database are running on the website? Please provide details:

13 Are there any important database, corporate network environment, critical data, critical systems, or critical applications connected to the backend of the public facing website, which is critical to the operation and function of the business? ○ Yes ○ No

If Yes, please provide details of these and how are they being secured:

DATA PROTECTION PROCEDURES

14 Is there a written data protection policy and privacy policy that applies to the Company? ○ Yes ○ No

If No, please provide details regarding data protection procedures for the Company:

15 Are all employees provided with a copy of, and required to comply with, the Company's data protection policy? ○ Yes ○ No

If Yes, how often are employees made to refresh knowledge of the company's data protection/privacy policy?

○ Quarterly ○ Biannually ○ Annually ○ Other (specify):

16 When were the Company's data protection and privacy policies last reviewed and by whom?

17 How often is the data protection/privacy policy reviewed and updated by a Data Security Officer or equivalent?

18 Does the Company's data protection policy comply with the data protection and privacy legislation applicable to all jurisdictions, industry standards and requirement in which the Company operates? ○ Yes ○ No

If No, please provide an explanation regarding non-compliance in applicable jurisdiction:

19 Does the Company transfer sensitive information across international borders? ○ Yes ○ No

If Yes, please explain how the company complies with local data privacy regulations when transferring sensitive information:

DATA/SYSTEMS – ACCESS, CONTROLS, PROTECTION & RECOVERY

20 Does the Company implement firewalls to prevent unauthorized access from external network connections to internal networks and computer systems? ○ Yes ○ No

If Yes, do all systems including computer systems, mobile devices and web servers operate behind Firewalled network connections? ○ Yes ○ No

21 Does the Company use anti-virus protections and procedures on all desktops, e-mail systems and mission critical servers to protect against viruses, worms, spyware and other malware? ○ Yes ○ No

If Yes, how often are such protections and procedures updated?

○ Quarterly ○ Biannually ○ Annually ○ Other (specify):

22 What type of endpoint protection solution is deployed?

○ XDR ○ EDR ○ Behavior Based Anti-virus ○ Signature Based Anti-virus ○ Other (specify):

23 Does the Company implement Intrusion Detection Systems (IDS) and have procedures in place to identify and detect network security weaknesses? ○ Yes ○ No

24 Does the company also implement Intrusion Prevention Systems (IPS) to stop detected incidents or malicious activities? ○ Yes ○ No

25 Does the Company monitor its network and computer systems for Breaches of Data Security, suspicious connections, or malicious IP addresses? ○ Yes ○ No

If Yes, please elaborate how this is carried out (for example: SIEM Tools, External Security Operations Centre [SOC] etc):

26 Does the company have physical security controls in place to prohibit and detect unauthorized access to their computer system and data center? ○ Yes ○ No

27 When was the last time the company conducted an IT security and what was the type of IT security audit conducted?

28 Has the Company conducted a Vulnerability Assessment & Penetration Test? ○ Yes ○ No

If Yes, was it conducted by an external vendor? ○ Yes ○ No

29 How frequent are Vulnerability Assessments & Penetration Tests conducted?

○ Quarterly ○ Biannually ○ Annually ○ Other (specify):

Please attach the summary of the findings, recommendations, and status of the implementation of the action plan to address the recommendations from the Vulnerability Assessment & Penetration Test reports.

30 Does the Company have encryption requirements for data-in-transit, data-at-rest and data in use to protect the integrity of Sensitive Data including data on portable media and cloud storage (e.g., laptops, DVD backup tapes, disk drives, USB devices, etc)? ○ Yes ○ No

If Yes, please describe where such encryption is used:

31 Does the Company have and maintain backup and recovery procedures for all:

Mission Critical systems? ○ Yes ○ No

Data and information assets? ○ Yes ○ No

If Yes, are they encrypted? ○ Yes ○ No

32 Does the company keep an offline backup or uses a cloud service designed for this purpose (i.e, the company maintains a backup that is disconnected from the company's network/ system/corporate environment)? ○ Yes ○ No

If Yes, how frequent is the company backing up their data offline? (Provide answer in number of hours)

33 Has an exercise been conducted to test successful restoration with such offline backup? ○ Yes ○ No

If Yes, when was such exercise last conducted?

34 Does the Company perform background checks on all employees and independent consultants? ○ Yes ○ No

35 Are required remote users authenticated before being allowed to connect to internal corporate networks and computer systems? ○ Yes ○ No

36 Is MFA/2FA implemented and enforced on all remote connections to internal corporate environment or cloud-based services? ○ Yes ○ No

If No, what measures are in place to prevent unauthorized access?

37 Is MFA/2FA implemented on all employees' user accounts and email accounts? ○ Yes ○ No

If No, what measures are in place to prevent unauthorized access?

38 Does the company have patching process in place for IT and operational technology (OT) systems, network infrastructure, software, application, and operating systems? ○ Yes ○ No

(a) If Yes, how often is patching carried out?

(b) If Yes, what is the company's target time to deploy "Critical (highest priority)" patches to both IT and OT (if any) Systems? Please state in number of hours:

39 Does the Company implement the following and how often are they updated?

Business Continuity Plan: ○ Yes ○ No Frequency updated:

Disaster Recovery Plan: ○ Yes ○ No Frequency updated:

If Yes, what is the Recover Time Objective (RTO) and Recovery Point Objective (RPO) for critical systems, data assets, IT and Operational Technology (OT) (if any) systems?

40 Does the company use any end-of-life or un-supported software/platform/products among all IT and Operational Technology (OT) (if any) systems? ○ Yes ○ No

If Yes, is it segregated from the rest of the network and not connected to the internet? ○ Yes ○ No

41 What measures are in place to mitigate the impact to the company's system or operation if there is a cyber incident?

42 Does the company use an e-mail filtering solution which blocks known malicious attachment and suspicious file types, including executables or suspicious messages based on their content or attributes of the sender? ○ Yes ○ No

If Yes, please describe what products or services are implemented.

43 Does the company conduct simulated phishing attacks? ○ Yes ○ No

If Yes, was the success ratio less than 15% on the last phishing exercise? (i.e, less than 15% of employees were successfully phished) ○ Yes ○ No

44 Please describe any additional steps taken by the organization to detect and prevent ransomware attacks (e.g, segmentation/ isolation of networks, additional software tools, external security services, phishing simulation, training and etc):

INTERCONNECTIVITY

45 Are all networks within the Company's offices/branches, entities or subsidiaries interconnected? ○ Yes ○ No

If Yes, please describe the measures are in place to isolate or contain an incident from affecting other connected segments within the network?

46 Is network segmentation implemented (i.e, is network segmented across geography, locations, business functions, departments and etc)? ○ Yes ○ No

47 Does the Company have internal network segmentation firewalls in place within their internal networks? ○ Yes ○ No

48 Please attach the corporate structure including all subsidiaries detailing the name of the entities, services and country where these entities are registered. Otherwise please indicate N/A if there are no subsidiaries: ○ Information attached ○ N/A

OUTSOURCING ACTIVITIES

49 Does the Company outsource any of its primary business functions to a third party? ○ Yes ○ No

If Yes, please indicate:

○ Human Resources ○ Customer Service ○ Marketing ○ Business Development ○ Information Technology

○ Internal Audit ○ Information Security ○ Network ○ Others (specify):

If Information Security applies, who is the security outsourced to?

Does the Company periodically audit the functions of the outsourcer to ensure that they follow the Company's security policies? ○ Yes ○ No

50 Does the Company outsource any data collection and/or data processing? ○ Yes ○ No

If Yes, please provide details of the data collection or data processing functions which are outsourced:

51 Does the Company require the entities providing data collection and/or data processing functions (Outsourcers) to maintain their own data protection liability insurance? ○ Yes ○ No

52 Does the Company require indemnification from Outsourcers for any liability attributable to them? ○ Yes ○ No

53 Does the Company share sensitive information with Outsourcers, suppliers or customers? ○ Yes ○ No

If Yes, are there any access rights restriction in place? Please provide details regarding access rights restriction:

54 How does the company manage and select Outsourcers?

55 Does the Company require all Outsourcers to comply with the terms of the Company's Data Protection Policy? ○ Yes ○ No

CLOUD SECURITY AND PROCEDURES

56 Does the Company use the Cloud? ○ Yes ○ No

If Yes, please answer questions 57 to 65 below. If No, proceed to the Network Failure section.

57 What procedures does the Company have in place to dictate which data may be stored in the Cloud?

58 Does the Company have any risk management procedures in place to deal with cloud storage? ○ Yes ○ No

59 Describe how the Company's organization is using cloud-based computing:

○ Community ○ Public ○ Private ○ Hybrid

(a) What Types of Services are being used or accessing the Cloud?

(b) What Types of Data are stored in the Cloud?

60 Has the Company undertaken due diligence to assess the security of the Cloud Provider and to confirm that the provider's practices comply with the applicable laws? ○ Yes ○ No

61 Where is the data stored and how it is secured?

62 Who is your cloud-based vendor (if any)?

63 If the cloud is interrupted, how will this affect the Company's business operations?

64 What co-operation and support are provided by the Cloud Provider in the event of a data breach? Which party incurs costs in the event of a data breach?

65 How does the Company's Business Continuity/ Disaster Recover Place address a cloud outage?

NETWORK FAILURE

66 Does the Company have a formal Data Security Program in place? ○ Yes ○ No

67 Does the Company have a Business Continuity / Disaster Recovery Plan in the event of a Network Failure? ○ Yes ○ No

If Yes, how often is the Company's Business Continuity / Disaster Recovery Plan reviewed and/or tested?

○ Quarterly ○ Half yearly ○ Annually ○ Every other year

68 Please describe what risk management procedures the Company has in place to prevent outages from occurring, including power back-up systems, fault tolerant data architecture, excess bandwidth for multiple providers, testing, change control procedures, risk assessment, etc:

69 Does the Company have protocols for the maximum lifecycles of system/network equipment within the organization? ○ Yes ○ No

If Yes, please provide further details below:

SOCIAL ENGINEERING

70 Does the Company apply 2FA when the users/customer/subscribers log-into the company system? ○ Yes ○ No

If No, please describe measures you have taken to avoid unathorised logins:

71 Are the duties below segregated so that no individual can control any of the following activities from commencement to completion without referrals to others?

(a) Amending funds transfer procedures: ○ Yes ○ No

(b) Opening new bank accounts: ○ Yes ○ No

(c) Awarding contracts following a tender: ○ Yes ○ No

If No to any of the above, please describe measures you have taken to avoid fraudulent banking or procurement activities:

72 With regards to funds transfer, please confirm at least two of the verifications below have been proceeded before any payment release:

(a) at their usual email or other internet messaging services; ☐ Yes ☐ No

(b) at their usual telephone number or VOIP; ☐ Yes ☐ No

(c) text message on their usual mobile number; or ☐ Yes ☐ No

(d) in-Person discussion: ☐ Yes ☐ No

If No, please describe measures you have taken to avoid fraudulent transfers:

NETWORK USAGE SYSTEM FRAUD

73 Has the Company ever sustained any loss through the usage fraud from a third party, or after enquiry of the Partners/Principals/Directors, is the Company aware of any circumstances which may give rise to a loss against the Company? ☐ Yes ☐ No

If Yes, please provide the relevant details and advise what precautions had been taken to prevent a recurrence:

74 Does the company use a password or a pass code to prevent unauthorized access to networked computer hardware or software, telephone system or internet system, and voicemails? ☐ Yes ☐ No

(a) If Yes, are all networked computer hardware or software, telephone systems or internet system; and voicemail accounts protected? ☐ Yes ☐ No

(b) How often are such protections updated? ☐ Daily ☐ Weekly ☐ Monthly ☐ Other (specify):

75 Are all employees provided with instructions how to protect their networked computer hardware or software, telephone system or internet system; and voicemail accounts? ☐ Yes ☐ No

If Yes, are all employees required to confirm compliance with all the procedures? ☐ Yes ☐ No

76 Does the company have a wi-fi connection? ☐ Yes ☐ No

(a) If Yes, is the connection password protected? ☐ Yes ☐ No

(b) How often are such protections updated? ☐ Daily ☐ Weekly ☐ Monthly ☐ Other (specify):

77 (a) Does the company monitor usage of networked computer hardware or software, telephone system or internet system; and voicemail accounts? ☐ Yes ☐ No

(b) And how does the company respond in the case of a breach of security?

78 How often is the company's usage of networked computer hardware or software, telephone system or internet system, and voicemail accounts last reviewed?

(a) ☐ Daily ☐ Weekly ☐ Monthly ☐ Other (specify):

(b) By whom?

INCIDENT INFORMATION

79 Has the Company been the subject of any investigation or audit in relation to data protection by a Data Protection Authority or other regulator? ☐ Yes ☐ No

If Yes, please provide full details:

80 Has the Company ever been subject to a Data Subject Access Request? ☐ Yes ☐ No

If Yes, please provide full details:

81 Has the Company ever been subject to an Enforcement Notice by a Data Protection Authority or any other regulator? ○ Yes ○ No

If Yes, please provide full details:

82 During the past three (3) years, has the Company experienced any occurrences, Claims or losses related to the Company's system failure or failure of the Cloud or does the Company have knowledge of a situation or circumstance which might otherwise result in a Claim against the Company with regard to issues related to the insurance sought? ○ Yes ○ No

If Yes, please provide full details:

83 Is there any other information in your possession material to an estimation of the risk to be Company and/or information of any nature which the underwriters should be made aware of? ○ Yes ○ No

If Yes, please provide full details:

INSURANCE HISTORY

84 Have you had similar insurance carried during the past three years? ○ Yes ○ No

If Yes, please provide details of your current Cyber Insurance policy:

Current insurer: Expiry Date:

Limit of indemnity: $ Excess: $ Premium: $

85 Have any claims been made against the Company or any of its former or current directors, officers, employees, subsidiaries or independent contractors with regards to the coverage sought in the past three years? ○ Yes ○ No

If Yes, please provided a detailed description of the circumstance:

86 Is the Company or any of its former or current directors, officers, employees, subsidiaries or independent contractors aware of any acts, errors, omissions or other circumstances, which may reasonably result in a claim relative to the insurance sought? ○ Yes ○ No

If Yes, please provided a detailed description of the circumstance:

COVER REQUIRED

87 Limit of indemnity required: ○ $1m ○ $2m ○ $5m ○ $10m ○ $15m ○ Other:

88 Level of excess required: ○ $5,000 ○ $10,000 ○ $15,000 ○ $20,000 ○ $50,000 ○ Other:

DECLARATION

On behalf of all proposed Applicants I/We declare and agree that all information provided in this proposal or attachments is true and correct in every respect and that all information that may be material in considering this proposal form has been fully and accurately disclosed to Delta Underwriting Private Limited in writing in a manner which would not mislead a prudent insurer.

Statement pursuant to Section 25(5) of the Insurance Act (Cap 142) or any amendments thereof; I/We agree that this declaration shall be the basis of and incorporated in the insurance contract and that the insurance contract may be avoided (amongst other things) if I/we fail to disclose in this application, fully and faithfully, all the facts which I/we know or ought to know.

I/We undertake to inform Delta Underwriting Private Limited of any material alteration to the above information whether occurring before or after the completion of this insurance contract. I/We understand that:

(a) I/We am/are obliged to advise Delta Underwriting Private Limited of any information which may be material to its consideration of this application. This information includes all information I/We know (or could reasonably be expected to know) which could influence the judgement of Delta Underwriting Private Limited whether or not to accept this application and (if accepted) on what terms, including cost and otherwise.

(b) Failure to provide this information may result in Delta Underwriting Private Limited refusing to provide the insurance.

(c) I/We have certain rights of access to and correction of this information.

Full name & title of individual:

Signature of Policyholder: Date:

RESET FORM SAVE AS PDF