ComTech

Combined liability and cyber insurance for information technology, media and telecommunications companies

Proposal Form

All questions must be answered giving full and complete answers.
Please ensure that this Proposal Form is Signed and Dated.
All fee or turnover declarations to be in Australian Dollars.

LAUW
LONDON AUSTRALIA UNDERWRITING

Suite 201, Level 2, 272 Pacific Highway
Crows Nest NSW 2065, Australia

www.lauw.com.au
t: 02 8912 6400

IMPORTANT NOTICES

Utmost Good Faith

In accordance with Section 13 of the Insurance Contracts Act 1984, the policy of insurance is based on utmost good faith requiring Underwriter(s) and the proposer/insured(s) to act towards each other with the utmost good faith in respect of any matter relating to the insurance contract.

Your Duty of Disclosure

Before you enter into an insurance contract, you have a duty to tell **Underwriters** anything that you know, or could reasonably be expected to know, may affect **Underwriters** decision to insure you and on what terms.

You have this duty until **Underwriters** agree to insure you.

You have the same duty before you renew, extend, vary or reinstate an insurance contract.

You do not need to tell **Underwriters** anything that:

- reduces the risk **Underwriters** insure you for; or
- is common knowledge; or
- **Underwriters** know or should know as an insurer; or
- **Underwriters** waive your duty to tell **Underwriters** about.

If You Do Not Tell Underwriters Something

If you do not tell **Underwriters** anything you are required to, **Underwriters** may cancel your contract or reduce the amount **Underwriters** will pay you if you make a claim, or both.

If your failure to tell **Underwriters** is fraudulent, **Underwriters** may refuse to pay a claim and treat the contract as if it never existed.

Claims Made

Insuring Clause 1 (Professional Indemnity) and Insuring Clause 3a (Cyber Liability) operate on a **claims** made and notified basis. This means that those insuring agreements provide you with cover for Claims first made against you and notified to **Underwriters** during the **Policy Period**.

The policy does not provide cover in relation to Known Facts (as set out in the relevant exclusion) nor in relation to any actual or alleged act, error, omission or other conduct which takes place before the Retroactive Date (if any) specified in the schedule.

Where you give notice in writing to us of any facts that might give rise to a claim against you as soon as reasonably practicable after you become aware of those facts but before the expiry of the **Policy Period**, you may have rights under Section 40(3) of the Insurance Contracts Act 1984 to be indemnified in respect of any claim subsequently made against you arising from those facts notwithstanding that the **Claim** is made after the expiry of the **Policy Period.** Those rights arise under the legislation only. The terms of the policy and the effect of the policy is that you are not covered for Claims made against you after the expiry of the **Policy Period**.

Privacy Notice

LAUW and **Underwriters** are committed to compliance with the provisions of the Australian Privacy Principles and the Privacy Act 1988 (Commonwealth). In order for **Underwriters** to assess the risk of and provide you with insurance products and assess and manage any claims under those products, it is necessary to obtain personal information from you. If you do not provide us with this information, this may prevent **Underwriters** from providing you with the products or services sought.

If you provide us with information about someone else, you must obtain their consent to do so.

LAUW and **Underwriters** may disclose your information to other insurers, their reinsurers, and insurance reference service or other advisers used by **Underwriters** or LAUW on behalf of **Underwriters** such as loss adjusters, lawyers or others who may be engaged to assist in claims handling, underwriting or for the purpose of fulfilling compliance and/or regulatory requirements. These third parties will all be contractually required to adhere to **Underwriters**' privacy obligations.

Our privacy policy contains information about how you can access the information we hold about you, ask us to correct and how you may make a privacy related complaint. For further details please see: http://lauw.com.au/privacy-policy.php

The above notes are not exhaustive and in no way should be read in isolation of the full policy terms, conditions, limitations and exclusions.

Section A: General Information

1.

Name of Company (Insured):

Principal Address:

Tel No:

Website(s) and estimated current monthly unique visitors:

Date of Establishment:

Number of employees:

Locations of overseas offices (please list countries):

2.

Describe in detail your business activities:

Do you anticipate any major changes in these activities in the forthcoming 12 months?

☐ **Yes** ☐ **No** If YES, please provide full details

3.

Please detail your turnover, including fees, for the past year, and estimated turnover for the current and next year:

Location	Past Year	Current Year (estimate)	Next Year (estimate)
Australia	$	$	$
New Zealand	$	$	$
USA	$	$	$
Rest of World (Please list countries):			
	$	$	$
	$	$	$
Total	$	$	$

Please provide a breakdown of your income generated in the last financial year as follows:

ACT	%	NSW	%	NT	%	QLD	%	Overseas	%
SA	%	TAS	%	VIC	%	WA	%	TOTAL	%

4.

Is the company part of any professional body or association?

☐ **Yes** ☐ **No** If YES, please detail below

5.

Does the company possess any professional accreditation?

☐ **Yes** ☐ **No** If YES, please detail below

6.

Has the company raised any external capital?

☐ **Yes** ☐ **No** If YES, please detail the investors and amounts

Section B: Organisational Governance

1.

Provide a category breakdown of your turnover:

	Past year (%)	Current year (estimate) (%)
Distribution or re-sale of third party hardware or third party shrink wrap software		
Manufacture or sale of own hardware or own shrink wrap software		
Sale of third party or own customisable software		
Hardware installation or maintenance		
Software installation or maintenance including configuration		
Bespoke software development or software customisation		
IT consultancy, training, project management and related support services		
Provision of contract staff		
Data processing		
Application service including Software as a Service (SaaS)		
Web hosting or data storage including provision of cloud services		
Telecommunication services including Internet Service provider (please complete Supplementary Telecommunications Questionnaire)		
Other (please detail each activity)		
TOTAL		

2.

What percentage of your turnover is paid to sub-contractors? ☐ %

What services do they provide for you?

Do you typically require such sub-contractors to carry Professional Indemnity Insurance?

☐ **Yes** ☐ **No** If YES for what limit?

If NO, why not?

3.

Do you provide products or services to the following industries?

		% of turnover
Banking / Financial institutions	☐ **Yes** ☐ **No**	%
Utilities	☐ **Yes** ☐ **No**	%
IT security	☐ **Yes** ☐ **No**	%
Logistics	☐ **Yes** ☐ **No**	%
Aerospace	☐ **Yes** ☐ **No**	%
Energy including oil & gas, nuclear activities	☐ **Yes** ☐ **No**	%
Medical / Healthcare	☐ **Yes** ☐ **No**	%
Public / Government	☐ **Yes** ☐ **No**	%

If YES to any of the above, please detail below

4.

Please list the five largest contracts undertaken during the last 3 years

Client	Industry	Nature of your product or service	Fee	Start date	End date
			$		
			$		
			$		
			$		
			$		

What is the average contract value per client?

$

Approximately how many clients do you have currently?

Please provide a breakdown of your client type?

Corporate %

Consumer %

What is the duration of your typical contract?

5.

What percentage of your contracts use your own standard delivery terms? %

Who approves variation from your own standard delivery terms?

Do your standard delivery terms:

Accept liability for consequential or indirect losses	☐ **Yes** ☐ **No**
Accept liability for financial damages greater than the value of contract	☐ **Yes** ☐ **No**
Include any form of liquidated damages	☐ **Yes** ☐ **No**
Warrant a performance standard greater than reasonable care and skill	☐ **Yes** ☐ **No**
Provide for an unlimited warranty period	☐ **Yes** ☐ **No**
Allow for changes to the scope of work without a written variation of contract	☐ **Yes** ☐ **No**
Provide indemnities to your clients (except Intellectual Property Rights, Death, Bodily Injury and/or Property Damage)	☐ **Yes** ☐ **No**

If YES to any of the above, please detail below

6.

If your product or service failed, which of the following would best describe the impact to your clients?

☐ No significant financial loss ☐ Non-immediate financial loss ☐ Immediate financial loss ☐ Immediate and significant financial loss

Please describe further

Section C: Products, Pollution and Public Liability

Do you require coverage for Products, Pollution, and Public Liability?

☐ **Yes** ☐ **No**

If Yes, please complete the following questions. If No, please skip to **Section D: Cyber**.

1.

Could the failure of your product or service result in:

The loss of life or bodily injury to a person

☐ **Yes** ☐ **No**

Damage or destruction to any physical property

☐ **Yes** ☐ **No**

If YES to any of the above, please detail below

2.

Do you manufacture or produce anything involving hazardous liquids, hazardous gases, or any other hazardous substances?

☐ **Yes** ☐ **No**

If YES to the above, please detail below

3.

What proportion of your work is carried out at the following locations?

Your own premises	Client's premises	Public areas
%	%	%

4.

What proportion of your products have been sold continuously for:

Less than 1 year	1-3 years	Over 3 years
%	%	%

5.

Please detail your procedure for testing your products and quality assurance?:

Section D: Cyber

Do you require coverage for Cyber?

☐ **Yes** ☐ **No** If Yes, please complete the following questions. If No, please skip to **Section E: Claims and Insurance History**.

1.

Do you hold personal information?

☐ **Yes** ☐ **No**

Personal information does not include information lawfully available to the general public for any reason, including information from foreign or local government records.

It does however include any information from which a person may be uniquely and reliably identified, including their name, telephone number, email address, tax file number, medicare number, medical or healthcare data or other protected health information, driver's license number or account number, credit card number, debit card number, access code or password that would permit access to that individual's financial account or any other non-public personal information as defined in any legislation or regulation (including amendments thereto) associated with personally identifiable financial, medical or other personal sensitive information, or any other legislation, regulation or by-law associated with identity theft or privacy.

Do you hold or process any of the following types of sensitive data?

	Yes/No	Approximate Number of Records
Financial information (excl credit/debit card records)	☐ **Yes** ☐ **No**	
Payment card information (credit/debit card records)	☐ **Yes** ☐ **No**	
Medical Information (such as Medicare of other personal healthcare data)	☐ **Yes** ☐ **No**	
Identity Information (including driver's licence, passport details)	☐ **Yes** ☐ **No**	
Name. addresses, telephone numbers	☐ **Yes** ☐ **No**	
Confidential intellectual property/trade secrets	☐ **Yes** ☐ **No**	

Do you anticipate any significant changes over the next 12 months for the above?

☐ **Yes** ☐ **No**

If Yes, provide full details

2.

What percentage of your turnover emanates from online or e-commerce activities?

%

What is the size of your dedicated IT budget annually?

3.

Can you confirm the company adheres to the following best practices and minimum security standards?

a) Have a dedicated individual responsible for Information Security and Privacy

☐ **Yes** ☐ **No**

b) Have a written incident management response plan

☐ **Yes** ☐ **No**

c) Does your Incident Response Plan reference mitigation steps for business continuity and recovery should a ransomware incident occur?

☐ **Yes** ☐ **No**

d) Perform background checks on all employees and contractors with access to sensitive data

☐ **Yes** ☐ **No**

e) Have restricted access to sensitive data (including physical records)

☐ **Yes** ☐ **No**

f) Have a process to delete systems access within 48 hours after employee termination

☐ **Yes** ☐ **No**

g) Have written information security policies and procedures that are reviewed annually and communicated to all employees including information security awareness training?

☐ **Yes** ☐ **No**

h) Ensure all remote access to IT systems is secure

☐ **Yes** ☐ **No**

i) Only use operating systems that continue to be supported by the original provider

☐ **Yes** ☐ **No**

j) You use anti-virus, anti-spyware and anti-malware software and update them regularly

☐ **Yes** ☐ **No**

k) You use firewalls and other security appliances between the Internet and sensitive data

☐ **Yes** ☐ **No**

l) You use intrusion detection or intrusion prevention systems (IDS/IPS) and these are monitored

☐ **Yes** ☐ **No**

m) Do you train end users against phishing and social engineering threats via ongoing campaigns and assessments?

☐ **Yes** ☐ **No**

o) You ensure all sensitive data on your system is encrypted

☐ **Yes** ☐ **No**

p) Do you enforce a BYOD (Bring Your Own Device) policy that ensures critical data is encrypted when transferred to portable media devices (USBs, Laptops etc.)?

☐ **Yes** ☐ **No**

q) You ensure all sensitive data on all removable media is encrypted

☐ **Yes** ☐ **No**

r) You ensure sensitive data is permanently removed (e.g. physical destruction not merely deleting) from hard drives and other storage media and from paper records prior to disposal

☐ **Yes** ☐ **No**

4.

1. Do you authenticate emails using:

☐ SPF (Sender Policy Framework), ☐ DKIM (DomainKeys Identified Mail), and/or ☐ DMARC (Domain-Based Message Authentication)?

2. Do you use O365 in your organisation?

☐ **Yes**. Have the following been implemented: ☐ MFA (multi factor authentication), ☐ ATP (advanced threat protection),

☐ Macros disabled by default

☐ **No**. Which product do you use for email monitoring (e.g. Proofpoint):

3. Do you allow local admin rights on workstations?

☐ **Yes** ☐ **No**

4. Do administrative/privileged accounts use a privilege access management (PAM) tool (e.g. CyberArk)?

☐ **Yes** ☐ **No.** Which product(s) do you use?

5. Do you use an endpoint protection (EPP) product?

☐ **Yes.** If so, which product(s)

☐ **No**

6. Have you deployed an endpoint detection and response (EDR) tool that covers 100% of:

☐ Servers and ☐ Endpoint? If so:

Which product(s):

If the EDR tool offers AI/automated rules based enforcement, has this been enabled?

☐ **Yes** ☐ **No** ☐ **N/A**

7. Does all remote access to your network and corporate email require multifactor authentication (MFA)?

☐ **Yes** ☐ **No**

8. Have you disabled remote desktop protocol (RDP)?

☐ **Yes** ☐ **No**

If No, have you implemented the following?

☐ VPN ☐ MFA ☐ RDP Honeypots

9. Do you operate a SIEM (Security information and event management) monitored 24/7/365 by an internal SOC (Security Operations Center) or MSSP (managed security service provide)?

☐ **Yes** ☐ **No**

10. Does your incident response plan (IRP) specifically address ransomware scenarios?

☐ **Yes** ☐ **No**

11. How frequently do you back up critical data?

☐ Daily ☐ Weekly ☐ Monthly ☐ Other, please explain below

12. Do you keep a copy of your critical backups offline and inaccessible from your network?

☐ **Yes** ☐ **No**

13. Which of the following are used to store backups?

☐ Cloud ☐ Secondary data centre ☐ Offline ☐ Within a separate network segment

14. Have the following been implemented to secure the backup environment?

☐ Segmentation ☐ Encryption ☐ MFA ☐ Vaulted Credentials

15. Do you use any commercial backup solutions (e.g.Commvault)?

☐ **Yes** ☐ **No.** Which product(s) do you use

16. Does your backup strategy include the use of immutable technologies?

☐ **Yes** ☐ **No**

17. Is the integrity of these backups and your recovery plans regularly tested?

☐ **Yes** ☐ **No**

If NO to any of the above, please detail below along with mitigating comments:

Please outline any additional controls your organisation has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, DNS, network segmentation, vulnerability scanning, phishing training):

5.

Are annual or more frequent internal/external audit reviews (including penetration testing) performed on your IT network and your procedures?

☐ **Yes** ☐ **No** If Yes, please provide a copy of the latest report from any examination/audit.

6.

a. Does the Insured have any exposure to the following critical vulnerabilities: CVE-2023-4966, CVE-2023-34362, CVE-2022-41010, CVE-2022-41082, CVE-2021-44228, CVE-2021-45046, CVE-2021-4104, CVE-2021-45105?

☐ **Yes** ☐ **No**

b. Would the Insured confirm whether they have enquired with IT providers they use, as to whether they have any exposure to this CVE, which may indirectly impact the Insured?

☐ **Yes** ☐ **No**

c. If the Insured has exposure to these CVEs, would they please confirm if any indicators of compromise have been identified?

☐ **Yes** ☐ **No**

d. If the answer to the above is "Yes", can Insured confirm what steps are being taken to remediate these vulnerabilities?

e. Has the insured installed the latest updates and patches wherever these critical vulnerabilities are known to be used?

☐ **Yes** ☐ **No**

f. To support the aforementioned patching, we would expect Insureds to investigate and discover unknown instances of critical vulnerabilities within their organisation (they should be scanning in order to do this, and ideally across 100% of their IT estate). Can the Insured advise whether or not they have actively investigated potential unknown instances of critical vulnerabilities and if so any outcome.

☐ **Yes** ☐ **No**

If YES, please provide details

g. If organisations do not already have such tools in place, they should deploy protective network monitoring and blocking tools, such as advanced endpoint monitoring (EDR), etc. Does the Insured currently utilise such defences?

☐ **Yes** ☐ **No**

h. In response to the critical vulnerabilities, has the Insured made any improvements or changes to their defences (Firewalls, scanning, EDR, IDS, monitoring activity etc.)?

☐ **Yes** ☐ **No**

Additional Comments

7.

Do you have a Disaster Recovery Plan (DRP) and/or Business Continuity Plan (BCP) in place?

☐ **Yes** ☐ **No**

If "Yes", please answer the following questions:

(a) In your DRP / BCP, how long would it take for you to be fully operational again following an incident?

(b) How often do you test your DRP / BCP?

8.

Please provide details of the vendors for the following services (or check box if it is managed and operated in-house):

	Vendor	In-house
Internet Service Provider		☐
Cloud / Hosting / Data Centre Provider		☐
Payment Processing		☐
Data or Information Processing (such as marketing or payroll)		☐
Offsite Archiving, Backup and Storage		☐

Section E: Claims and Insurance History

1.

Have you previously been insured for your Technology E&O, Products, Pollution and Public Liability and Cyber risks?

☐ **Yes** ☐ **No**

If Yes, please provide the following **unless you are currently insured with LAUW**

Limit of Indemnity:

Insurer:

Excess:

Expiry Date:

Premium:

2.

Limit of indemnity required:

Excess required:

3.

Do you have any overdue contracts, overdue or disputed clients fees, or unpaid client invoices?

☐ **Yes** ☐ **No** If Yes, provide full details

4.

Are you aware of any other insurance that is in place that cover the risk(s) proposing to be insured by completing this application (including insurance cover in place for sub-contractors engaged by you)?

☐ **Yes** ☐ **No** if yes, please provide a copy of the relevant certificates of currency of those policies.

5.

Regarding all the types of insurance covers to which this Proposal Form relates, are you or any of the Partners, Principals, or Directors, after having made full enquiries, including of all staff, aware of any of the following matters?

Any claims (successful or otherwise) or cease and desist orders been made against the company, its predecessor, or present or past Partners, Principals, or Directors

☐ **Yes** ☐ **No**

Any circumstances which may give rise to a claim against the company, its predecessor or any past or present Partner, Director, Principal or employee

☐ **Yes** ☐ **No**

The receipt of any complaints, whether oral or in writing, regarding services performed, products or solutions sold or provided, or advice given by you

☐ **Yes** ☐ **No**

Any loss or damage that has occurred to the company or its predecessor

☐ **Yes** ☐ **No**

Any privacy breach, virus, DDOS, or hacking incident which has, or could, adversely impact(ed) your business

☐ **Yes** ☐ **No**

Any unforeseen down time to your website or IT network of more than 3 hours

☐ **Yes** ☐ **No**

If YES to any of the above, please provide full details

I/We declare that the above answers, statements, particulars and additional information are true to the very best of our knowledge and belief. After full enquiry, I/We also confirm that I/We have disclosed all information and material facts that may alter the Underwriters' view of the risk, or affect their assessment of the exposures they are covering under the policy. I/We understand that all answers, statements, particulars and additional information supplied with this proposal form will become part of and form the basis of the policy.

I/We acknowledge that we have read and understood the content of the Important Notices contained in this proposal.

Signed: SIGN

Date:

Position:

For and/on behalf of the Proposer:

Name in capital letters (printed):

Supplementary Telecommunications Questionnaire

Please only complete the following questions if you have declared turnover arising from Telecommunication services including Internet Service Provider under Question 1 of **Section B: Technology E&O**

1.

Are you a telecommunications company?

☐ **Yes** ☐ **No** If YES, what percentage of your turnover emanates from telecommunications services? ____ %

Do you provide any of the below services? If yes, please tick

☐ Voice communication ☐ Internet Service Provision ☐ Data communication

☐ Content / Media Provision ☐ Other (please detail) ____

2.

Do you provide or carry out any of the following?		**% of turnover**
Re-sell third party telecommunication company's services	☐ **Yes** ☐ **No**	%
Telecommunications related project management	☐ **Yes** ☐ **No**	%
Telecommunications related consultancy	☐ **Yes** ☐ **No**	%
Any other telecommunications related services (detail below)	☐ **Yes** ☐ **No**	%

3.

Please provide the following breakdown of your clients:	**Corporate**	**Consumer**
Number of customers		
Number of telephone access lines provided (fixed lines)		
What percentage of your fixed lines are:		
• **Analogues**	%	%
• **Digital (ISDN)**	%	%
• **IP enabled (non-hosted)**	%	%
• **IP enabled (hosted)**	%	%
• **Hybrid**	%	%
• **Other (please detail)**	%	%
Number of telephone access lines provided (mobile)		

4.

Do you outsource customer billing to a third party provider?

☐ **Yes** ☐ **No** If YES, please name the provider

5.

In the course of your business, are you involved in security solutions? (including in respect to "phreaking")

☐ **Yes** ☐ **No** If YES, please explain the extent of your involvement and any areas of specialism

6.

Please describe below how you assist your clients with managing any toll fraud or "phreaking" exposure?

For example: flagging unusual call usage patterns, account block, or similar