PROPOSAL FORM ➲

Cyber Proposal Form $0-$65M Revenue

EXTF213

Refer to page 4 for Glossary of Terms

Insured Name

Insured Name _____

Trading Name _____

Client Website URL_____

ABN_____

Insured Location_____

Insured Details

Annual Revenue $_____

Type of Trade _____

Do you conduct business in more than one state? Yes ◯ No ◯

Do you generate any revenue from subsidiaries or overseas? Yes ◯ No ◯

If 'Yes', please provide more information below

_____

Is your business a franchisee or part of a larger group of companies? Yes ◯ No ◯

Cyber Security Details

1. **Do you deploy an active business grade firewall at all external gateways of your network and an active business grade antivirus application across your entire network, including servers or endpoints?** Yes ◯ No ◯
2. **Do you (or your IT service provider) backup your data to an isolated environment at least every 7 days and test it at least every 365 days?** Yes ◯ No ◯
3. **Do you secure all remote access to your network with a minimum of multifactor authentication?** Yes ◯ No ◯
4. **Do you install critical patches within 30 days of release?** Yes ◯ No ◯
5. **Have you suffered any loss or has any claim been made against you or are you aware of any matter that is reasonably likely to give rise to any loss or claim in the last 36 months where you would seek an indemnity from our cyber insurance policy?** Yes ◯ No ◯

   If 'Yes', please provide more information below

_____

ATC Insurance Solutions Pty Ltd. Level 4, 451 Little Bourke Street, Melbourne Vic 3000 Telephone (03) 9258 1777 Email cyber@atcis.com.au Web www.atcis.com.au

6. **Do you provide, maintain or operate any cloud, web or data hosting services to or on behalf of third parties?** Yes ◯ No ◯

7. **Does the Insured have any financial nexus, financial agreements or contractual associations to Russia, Ukraine or Belarus?** Yes ◯ No ◯

   This is an exclusion on all cyber policies.

$30M-$65M Revenue

8. **Is all Personal data on individuals (PCI, PII, PFI and / or PHI) encrypted whilst on, and in transmission from, your network?** Yes ◯ No ◯

9. **Have you disabled Remote Desktop Protocol (RDP) on all your network's endpoints, including servers, unless protected by MFA?** Yes ◯ No ◯

Funds Transfer Fraud Sub-Limit

Is this sub limit required? Yes ◯ No ◯

Sub Limit Option $_____

10. **Do you have a written procedure whereby, all new (including changes to existing) payment details or contact details are confirmed by an alternative method to the original method used, before any payment is made?** Yes ◯ No ◯

11. **Do you maintain procedures, at least annually, for the provision of written training materials to all employees relating to the dangers of social engineering fraud, phishing and cyber fraud?** Yes ◯ No ◯

Policy Period

Policy Inception Date _____/_____/_____ **Policy Expiry Date** _____/_____/_____

Which policy limit would you like? ◯ $100,000 ◯ $250,000 ◯ $500,000 ◯ $1,000,000 ◯ $2,000,000

PROPOSAL FORM ➲ Declaration and Signature

Please read carefully the following important information before signing:

DUTY OF DISCLOSURE

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

You have this duty until we 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 us anything that:

- reduces the risk we insure You for; or
- is common knowledge; or
- we know or should know as an insurer; or
- we waive Your duty to tell us about.

If You do not tell us something

If You do not tell us anything You are required to, we may cancel Your contract or reduce the amount we will pay You if You make a claim, or both. If Your failure to tell us is fraudulent, we may refuse to pay a claim and treat the contract as if it never existed.

Privacy

In this statement "we", "us" and "our" means Lloyd's and ATC Insurance Solutions (ATC) as its agent.

We are bound by the requirements of the *Privacy Act 1988* (Cth), the *Privacy Amendment (Private Sector) Act 2000* (Cth) and the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*. This sets out standards on the collection, use, disclosure and handling of personal information.

Our Privacy Policy is available at www.atcis.com.au or by calling 03 9258 1777.

We, and our agents, need to collect, use and disclose your personal information in order to consider your application for insurance and to provide the cover you have chosen, administer the insurance and assess any claim. You can choose not to provide us with some of the details or all of your personal information, but this may affect our ability to provide the cover, administer the insurance or assess a claim.

We may disclose your personal information to third parties (and/or collect additional personal information about you from them) who assist us in providing the above services and some of these are likely to be overseas recipients in the United Kingdom. These parties which include our related entities, distributors, agents, insurers, claims investigators, assessors, lawyers, medical practitioners and health workers, and federal or state regulatory authorities, including Medicare Australia and Centrelink will only use the personal information for the purposes we provided it to them for (unless otherwise required by law).

Information will be obtained from individuals directly where possible and practicable to do so. Sometimes it may be collected indirectly (e.g. from your representatives or co-insureds). If you provide information for another person you represent to us that:

- you have the authority from them to do so and it is as if they provided it to us;
- you have made them aware that you will or may provide their personal information to us, the types of third parties we may provide it to, the relevant purposes we and the third parties we disclose it to will use it for, and how they can access it. If it is sensitive information we rely on you to have obtained their consent on these matters. If you have not done or will not do either of these things, you must tell us before you provide the relevant information.

You are entitled to access your information and request correction if required. You may also opt out of receiving materials sent by us by contacting ATC on (03) 9258 1777 or write to us at the address given on page 1.

Claims made during the period of insurance

This policy provides cover on a "claims made" basis, which means that claims first advised to you (or made against you) during the period of insurance are covered, irrespective of when the incident causing the claim occurred. When you give notice in writing to us of facts that might give rise to a claim against you and you give that notice as soon as reasonably practicable after you become aware of those facts but before the cover provided by your insurance contract with us expires, we cannot refuse to cover you by reason only of the fact that the claim against you is actually made after that expiry date.

Subrogation

This policy contains provisions which have the effect of excluding or limiting the insurer's liability in respect of a loss where you have prejudiced the insurer's rights of subrogation where you are a party to an agreement which excludes or limits insurer's rights to recover the loss from another party. You are hereby notified of the effect of these provisions.

Declaration

I/We represent that the above statements and facts are true and that no material facts have been suppressed or misstated.

Furthermore, I/we

1. **have either completed all of the questions on this form personally or they have been completed by someone else on my/our behalf and the answers have been checked for fullness and accuracy by me/us**
2. **have read and understood the information concerning the duty of disclosure and all other important notices;**
3. **agree to ATC Insurance Solutions obtaining from my/our previous insurer(s) any information it may need about my/our claims or insurance history;**
4. **agree to ATC Insurance Solutions making enquiries from any third party to verify my/our claims history and other information disclosed herein or statements made by myself/ourselves in making this application;**
5. **agree to ATC Insurance Solutions disclosing to any insurance intermediary appointed or toany former or future insurer of myself/ ourselves the claims history or any other information as may be determined;**
6. **have received and read a full copy of the Product Disclosure Statement for this insurance with this application form.**

If insufficient space is provided on this proposal in respect of any questions contained on the proposal, please attach a sheet of paper containing the additional information, noting the relevant question number and sign and date such attachment.

I/We declare that the answers given herein are in every respect true and correct and that

I/We have not withheld any information likely to affect the acceptance of the Proposal.

I/We have read and understood the Proposal and the Policy conditions.

Signature_____

Name_____

Date _____/_____/_____

Business Grade Antivirus

Advanced antivirus solutions designed for businesses to protect their systems from malware, viruses, and other cyber threats. These solutions offer enhanced features such as centralised management, real-time threat detection, and comprehensive reporting capabilities.

Business Grade Firewall

Advanced firewall solution designed for businesses to protect their networks from unauthorised access, cyber threats, and data breaches. These firewalls offer enhanced features such as intrusion detection and prevention, VPN support, and robust traffic management capabilities.

IT Service Provider

Any third party with whom the Insured has a written contract for the provision of computing services, IT systems platforms or IT business applications including infrastructure management, software development, network security, technical support, and cloud services.

Cloud, Web, or Data Hosting Services

Services that provide storage, processing, and management of data, applications, and websites on remote servers accessed via the internet. These services enable organisations to host their digital assets without the need for on-premises infrastructure.

Data Back Up

The process of copying and storing data to ensure it can be recovered in the event of data loss, corruption, or disaster. Regular backups are essential for data integrity and business continuity.

Critical Patches

Updates released by software vendors to fix vulnerabilities that could be exploited by malicious actors. These patches are deemed critical due to the severity of the vulnerabilities they address and the potential impact on the organisation if left unpatched.

Critical Systems

Systems that are essential to the operation of an organisation. These systems must be protected and maintained to ensure business continuity and operational efficiency.

Data Encryption

The process of converting data into a coded format to prevent unauthorized access. Only those with the decryption key can read the encrypted data, ensuring its confidentiality and security.

Employee Awareness

Training programs designed to enhance employees' security awareness, such as identifying potential phishing emails.

Endpoint Protection

Software installed on individual computers (endpoints) that uses behavioural and signature-based analysis to detect and stop malware infections.

Endpoints

Devices such as computers, laptops, smartphones, and tablets that connect to and communicate with a network. Endpoints are often targeted by cyber threats and require protection through security measures like antivirus software and endpoint protection solutions.

External Gateway

A network node that serves as an access point to another network, often the internet. External gateways manage and control the flow of data between internal networks and external networks, providing security and connectivity.

Funds Transfer Fraud

A type of cybercrime where attackers deceive individuals or organisations into transferring money to fraudulent accounts. This often involves phishing or social engineering tactics.

Multi-Factor or 2 Factor Authentication (MFA/2FA)

A security process where a user authenticates themselves through two different means when remotely logging into a computer system or web-based service, typically using a password and a passcode generated by a physical token device or software.

Phishing

A cyberattack method where attackers send fraudulent messages, often via email, that appear to come from a reputable source. The goal is to steal sensitive data such as login credentials or to install malware on the victim's device.

Security Awareness Training

Programs aimed at educating employees about the importance of security practices and how to recognise and respond to potential security threats.

Servers

Computers or systems that provide resources, data, services, or programs to other computers, known as clients, over a network. Servers are critical components of IT infrastructure and require robust security measures to protect against cyber threats.

Social Engineering

A tactic used by cybercriminals to manipulate individuals into divulging confidential information. Social engineering exploits human psychology rather than technical hacking techniques.