PROPOSAL FORM

emergence

tech event protection

Use this proposal form if:

- you are in the IT, internet or telecommunications industry, and
- you are applying for our IT liability package policy which combines Professional Indemnity, Cyber, and Public and Product Liability coverage.

Completing this form requires technical knowledge of your IT.
Consult with your IT manager or head of cyber security as necessary.

GENERAL

Name of policyholder:

New Zealand Business Number (NZBN):

Year of establishment:

Is the policyholder a subsidiary, franchisee or part of a larger group? ☐ Yes ☐ No

If Yes, please provide details:

Policyholder's principal address:

Website(s) or domain(s):

List all websites or domains:

or confirm: Don't know /don't have a website, domain or business email: ☐

Note: If cyber cover is elected, we will provide "smarter cyber" monitoring for your websites and domains.

Please provide the contact details of the person who is responsible for cyber security:

Note: This information will be used to provide critical security updates on a needs basis and will not be used for marketing purposes.

Name	Title
Email	Mobile

Total number of employees:

TRADING NAMES, SUBSIDIARIES, AFFILIATES, JOINT VENTURE OR CONSORTIUM

If you wish to list trading names, please list them individually in the boxes provided below:

Name all subsidiaries, including all overseas subsidiaries, you wish to include:

Subsidiary Name	Location	Revenue Contribution
		%
		%
		%
		%

PROPOSAL FORM

emergence

tech event protection

TRADING NAMES, SUBSIDIARIES, AFFILIATES, JOINT VENTURE OR CONSORTIUM

Name all joint ventures and consortiums you wish to include:

Name of Joint Venture or Consortium	Business Activity	Revenue
		$
		$

Name all affiliated companies you wish to include:

Name of Affiliated Company	Business Activity	Relationship	Revenue
			$
			$

MERGERS AND ACQUISITIONS (M&A)

Have you made any acquisitions or merged with another company in the past 18 months? ☐ Yes ☐ No

If Yes, please provide details below:

Name of entity 1:		**Date of M&A:**	
Business activity:		**Revenue:**	$

Please select the most appropriate answer below:

☐ Acquired company will run entirely separately or there is no plan to integrate

☐ Still in the process of integrating the acquired company

☐ Acquired company has been fully integrated into existing business and shares the same infrastructure, resources, and policies

Name of entity 2:		**Date of M&A:**	
Business activity:		**Revenue:**	$

Please select the most appropriate answer below:

☐ Acquired company will run entirely separately or there is no plan to integrate

☐ Still in the process of integrating the acquired company

☐ Acquired company has been fully integrated into existing business and shares the same infrastructure, resources, and policies

FINANCIALS

Estimated revenue for the coming 12 month period by territory:		Are you located in the territory?
Australia/NZ	$	☐ Yes ☐ No
EU/UK	$	☐ Yes ☐ No
USA	$	☐ Yes ☐ No
Rest of world	$	☐ Yes ☐ No
Total	$	

How many of the last 3 years have you posted a net profit?

☐ 0 ☐ 1 ☐ 2 ☐ 3

Continued overleaf

PROPOSAL FORM

tech event protection

emergence

CURRENT INSURANCE

Are you currently insured under a technology insurance policy? ☐ Yes ☐ No

If yes, please provide details of your current insurance policy:

Coverage	Limit	Excess	Insurer	Premium
Professional Indemnity	$	$		$
Cyber	$	$		$
Public and Product Liability	$	$		$

BUSINESS ACTIVITIES

1. Please provide a detailed description of your business activities:

2. Please provide an approximate percentage of revenue derived from each of the following categories:

Sales of own pre-packaged software	%	Manufacture or sale of own hardware	%
Sales of third-party pre-packaged software	%	Sales of third-party hardware	%
Sales of third-party customised software	%	Contract manufacturing services	%
Custom software or programming services	%	Product assembly services	%
IT project management services	%	Product design and prototyping services	%
General IT consulting services	%	Product maintenance and repair services	%
IT security consulting services	%	Telecommunication and internet services	%
Software as a Service (SaaS) or Platform as a Service (PaaS)	%	Sales of third-party cloud, network or hosting services	%
Integration or implementation services	%	Operation of cloud, network or hosting services	%
Managed services	%	IT staff recruitment or staff placement	%
Managed security services	%	Website design and development services	%
IT Helpdesk, training, & maintenance services	%	Other: (note: including any non-IT services or products)	%

PRODUCT AND SERVICE APPLICATION

3. If your product or service is being used in any of the following industries, please provide details:

End use of product / service:	Details of the product or service provided:	% of revenue
Adult content		%
Aerospace / Airline / Automotive		%
B2C e-Commerce		%
Cryptocurrencies / Non-fungible tokens (NFT)		%
Gambling systems		%
Healthcare / medTech		%
Military guidance and weaponry		%
Payment processing / gateway		%
PLC / SCADA / OT		%
Public transportation		%
Safety critical systems		%
Social media		%
Trading / Exchange platform		%
Utilities		%

Additional details:

SUBCONTRACTORS

4. Approximate percentage of work that is carried out by subcontractors: %

5. Do you have a training or onboarding process for all your subcontractors? ☐ Yes ☐ No

6. Do you have a quality assurance process for all your subcontractors? ☐ Yes ☐ No

7. Do you require subcontractors to carry their own insurance? ☐ Yes ☐ No

8. Do you maintain your rights of recovery or subrogation against your subcontractors? ☐ Yes ☐ No

9. Describe the type of work that you subcontract to others:

Continued overleaf

CONTRACT AND RISK MANAGEMENT

10. Please provide details of your four largest contracts:

Client Name:	Contract Size	Nature of work	Development / Integration Period	Maintenance / Licensing Period	Total
	$		months	months	months
	$		months	months	months
	$		months	months	months
	$		months	months	months

11. Do you always use a written contract of agreement with all your clients? Yes No

12. What is the average size of your active contracts? $

13. What is the average length of your active contracts? months

14. Approximate percentage of active contracts on your own standard contract template: %

15. Have your standard contract templates or terms of service been reviewed by a legal counsel? Yes No

16. Do you seek legal review prior to entering contracts that are on client's contract templates or substantially customised from your standard contract template? Yes No

17. Approximate percentage of fixed price contracts: %

18. How often do you exclude consequential / indirect losses in a contract? %

19. How often do you limit your liability to 12 months of contract value or less in a contract? %

20. What is the maximum liability you have agreed to in your current active contracts? $

21. How often do you agree to liquidated damages or a penalty clause in a contract? %

22. How often do you agree to hold harmless or indemnify your clients in a contract? %

23. Are scope of work, specifications, responsibilities, and deliverables clearly defined in contracts? Yes No

24. Do you require all requests for change to be formally agreed and signed-off by both parties? Yes No

25. Do you require customer sign-off upon completion of project/product/service? Yes No

QUALITY CONTROLS

26. Do you have written quality control procedures in place? Yes No

27. Do you keep records of issues or downtime, identify the root cause, and any preventative measures to avoid similar situations in the future? Yes No

28. Do you have a formal procedure to handle customers' complaints or dissatisfaction? Yes No

29. Please list the industry standard certifications you have achieved:

QUALITY CONTROLS (CONT.)

30. Do you do custom software or system development projects? If yes, please answer below:	Yes No
Do you have a formalised written system development methodology?	Yes No
Do you have a formal testing and acceptance procedure in place?	Yes No
Do you have a formal procedure to review milestones or deliverables?	Yes No
Do you incorporate security into your development process, i.e. DevSecOps?	Yes No
31. Do you manufacture tangible product or you have a third-party manufacture on your behalf? If yes, please answer below:	Yes No
Do you have a written product or prototype development protocols in place?	Yes No
Do you have a formal quality control and quality assurance procedures in place?	Yes No
Do you have a formal sign-off process for product design prior to manufacturing?	Yes No
Is your product user manual and product warranty vetted by a legal professional?	Yes No

INTELLECTUAL PROPERTY (IP)

32. Do you consult a legal professional prior to release of a new product?	Yes No
33. Do you have a formal procedure to safeguard against infringing IP rights of others?	Yes No
34. Do you perform infringement clearance searches for all trademarks, copyrights, or patent rights?	Yes No
35. Do you have procedures to secure rights or written consent to use third-party IP?	Yes No
36. Is the original source code documented properly in a logbook or by other means?	Yes No

37. What percentage of your revenue is derived from products or software that are:

less than 1 year old: % 1 to 3 years old: % over 3 years old: %

38. List all IP rights that you hold for your products (including patent rights, trademarks, copyrights, designs, etc) or confirm you do not hold any IP rights

Number / Identifier	Title / Details	Territory

39. Are you currently involved in an intellectual property rights dispute?	Yes No
40. Are you aware of a third-party breaching your intellectual property rights?	Yes No

MULTIMEDIA

41. Do you have a formalised written social media policy?	Yes No
42. Do you have all your content reviewed by qualified personnel prior to publication?	Yes No
43. Do you host third-party content on your website?	Yes No
44. Do you have a procedure to secure rights or written consent to use third-party content?	Yes No
45. Do you monitor your content and publications for potentially offensive, libel, slander, damaging or infringing materials?	Yes No

APPLICATIONS, SYSTEMS, AND DELIVERY

46. Please list the applications or systems you rely on most for the course of your business:

Application / System	Name of IT Provider	Recovery Point Objective	Recovery Time Objective
		hours	hours
		hours	hours
		hours	hours
		hours	hours

47. Do you offer Software as a Service (SaaS), Platform as a Service (PaaS), network or hosting services to your customers? ☐ Yes ☐ No

If yes, how is this delivered or hosted? (tick all that apply)

☐ on your own network ☐ on-premises on customer's network ☐ on third-party vendor network

48. Are you responsible for the system and data security? ☐ Yes ☐ No

49. Do you segregate your network to prevent a scenario where one downtime or one cyber event affects all customers? ☐ Yes ☐ No

50. Do you have redundancy or failover procedures in place to ensure continuation of service in the event the main server fails? ☐ Yes ☐ No

DATA PROTECTION

51. Do you collect, process, hold or store data on behalf of any third-party? ☐ Yes ☐ No

52. Please state the estimated total number of Personally Identifiable Information (PII) and other sensitive records you collect, process, hold or store in your business, including on behalf of others.

Note: All categories of PII relating to the same individual (whether active or inactive) should only count as a single unique record.

☐ 0 – 25,000 ☐ 25,001 – 50,000 ☐ 50,001 – 75,000 ☐ 75,001 – 100,000

☐ 100,001 – 200,000 ☐ 200,001 – 300,000 ☐ 300,001 – 400,000 ☐ 400,001 – 500,000

☐ 500,001 – 750,000 ☐ 750,001 – 1,000,000 ☐ 1,000,001 – 1,500,000 ☐ 1,500,001 – 2,000,000

☐ 2,000,001 – 2,500,000 ☐ 2,500,001 – 5,000,000 ☐ >5,000,000

If > 5,000,000 please provide total number: ____________

53. Please select the type of records collected, processed, held or stored: (tick all that apply)

Customer information (e.g. name, address, email address, phone number etc)	☐ Yes ☐ No
Payment card information	☐ Yes ☐ No
Identity information (e.g. driver's licence, tax file number, passport number etc)	☐ Yes ☐ No
Banking or financial information	☐ Yes ☐ No
Medical or healthcare information	☐ Yes ☐ No
Biometric data	☐ Yes ☐ No
Trade secrets or intellectual property	☐ Yes ☐ No

Continued overleaf

DATA PROTECTION (CONT.)

54. Do you protect all personally identifiable information and other sensitive data through encryption while:

(tick all that apply)

At rest	☐ Yes	☐ No
Backed up	☐ Yes	☐ No
In transit	☐ Yes	☐ No
Stored on portable devices	☐ Yes	☐ No
Stored with third parties	☐ Yes	☐ No

55. Do you have the following policies in place? (tick all that apply)

☐ Privacy policy ☐ Cookies policy ☐ Data retention and data destruction policy

☐ Bring your own device policy that ensures data on portable devices is encrypted

GOVERNANCE

56. How frequently do you provide security awareness training to your employees?

☐ Annually ☐ Quarterly ☐ Monthly ☐ Not Provided

57. How frequently do you test employees' security awareness through simulated phishing campaigns?

☐ Annually ☐ Quarterly ☐ Monthly ☐ Not Provided

ASSET SECURITY

58. Do you maintain an inventory of all your hardware and software?

Hardware	☐ Yes	☐ No
Software	☐ Yes	☐ No

59. Have you implemented secure configurations to all hardware and software assets? ☐ Yes ☐ No

If Yes, please indicate which of the following have been implemented:

(tick all that apply)

Changing and/or disabling default accounts and passwords	☐ Yes	☐ No
Disabling or removing unneeded services, components or features	☐ Yes	☐ No
Implementing vendor specific security recommendations	☐ Yes	☐ No
Enforcing encryption of local storage devices	☐ Yes	☐ No
Enable appropriate backups	☐ Yes	☐ No
Configure logging of system logons, activity, warnings and errors	☐ Yes	☐ No
Sending all logs to a centralised logging server	☐ Yes	☐ No
Assets are onboarded onto EDR and/or SIEM platforms	☐ Yes	☐ No

60. Have you deployed an Endpoint Detection and Response (EDR) tool on Servers?

☐ Yes, EDR covers 100% ☐ Yes, EDR covers less than 90%

☐ Yes, EDR covers 90% or more ☐ No, we have not deployed an EDR tool

Continued overleaf

ASSET SECURITY (CONT.)

61. Have you deployed an Endpoint Detection and Response (EDR) tool on Endpoints?

- ☐ Yes, EDR covers 100%
- ☐ Yes, EDR covers less than 90%
- ☐ Yes, EDR covers 90% or more
- ☐ No, we have not deployed an EDR tool

Indicate if AI/automated rules-based enforcement has been enabled: ☐ Yes ☐ No

If EDR has not been deployed or covers less than 90%, indicate what compensatory measures you have implemented: (tick all that apply)

Application whitelisting	☐ Yes	☐ No
Endpoint Protection Platform (EPP)	☐ Yes	☐ No
Next Generation Firewall (NGFW)	☐ Yes	☐ No
Intrusion Detection/Prevention System (IDS/IPS)	☐ Yes	☐ No
Content control software (web/URL filtering)	☐ Yes	☐ No
Other (please provide details below):	☐ Yes	☐ No

62. Have you implemented a critical security patch management process for your IT systems? ☐ Yes ☐ No

If Yes, how do you handle security patches?

- ☐ Manual updates, implemented within 30 days
- ☐ Manual updates, implemented within 90 days
- ☐ Manual updates, no time frame for implementation
- ☐ Devices are set to update software automatically (where available)

EMAIL SECURITY

63. Do you use an email filtration and scanning tool to authenticate emails and flag and quarantine suspicious content (e.g. executable files)? ☐ Yes ☐ No

64. Do you tag external emails to alert employees that the email originated from outside the organisation? ☐ Yes ☐ No

IDENTITY AND ACCESS MANAGEMENT

65. Do you restrict user access based on role or job function? ☐ Yes ☐ No

66. Do you terminate user access upon termination of employment? ☐ Yes ☐ No

Continued overleaf

IDENTITY AND ACCESS MANAGEMENT (CONT.)

67. Is Multi-Factor Authentication (MFA*) required for all users to access the following systems/platforms/services?

All remote access to the network?	Yes	No
Web-based email?	Yes	No
Admin/privilege service accounts?	Yes	No
Cloud resources, including back-ups?	Yes	No

***Note:** To qualify as multi-factor authentication, the authentication mechanism needs to be knowledge (something the user and only the user knows) and possession (something the user and only the user has). That way the compromise of any single device will only compromise a single authentication factor.

ASSESSMENTS

68. In the last 12 months have you had any of the following conducted on your business/systems?

Penetration test	Yes	No
Vulnerability scan	Yes	No
Payment Card Industry (PCI) assessment	Yes	No
External IT audit	Yes	No

END OF LIFE TECHNOLOGY

69. Do you rely on any operating system, software or hardware that is no longer supported or is considered end of life by the manufacturer? Yes No

If Yes, please answer the following questions:

Is any end of life technology internet facing?	Yes	No
Is it segregated from the rest of the network?	Yes	No
Has additional support been purchased where available?	Yes	No

Please outline any additional security measures that have been implemented to prevent exploitation of any vulnerabilities:

Please provide an estimated timeline for you to phase out the use of end of life technology:

RESILIENCY AND RECOVERY

70. How frequently do you backup your critical data and systems?
   - [ ] Daily [ ] Weekly [ ] Monthly [ ] Greater than Monthly

71. Do you keep a copy of critical backups offline, segregated from and inaccessible to your network? [ ] Yes [ ] No

72. Is your backup environment: (tick all that apply)

In the cloud	[ ] Yes	[ ] No
On premises	[ ] Yes	[ ] No
At a secondary, offsite data centre	[ ] Yes	[ ] No
Encrypted	[ ] Yes	[ ] No
MFA protected	[ ] Yes	[ ] No
Using immutable technology	[ ] Yes	[ ] No

73. How frequently do you test system restoration capabilities by performing a full restoration from a sample set of backup data?
   - [ ] Annually [ ] Quarterly [ ] Monthly [ ] Not tested

74. Please confirm which of the following formal plans you have in place and whether tested at least annually:

	In Place?		Tested annually?	
Disaster Recovery Plan (DRP)	[ ] Yes	[ ] No	[ ] Yes	[ ] No
Business Continuity Plan (BCP)	[ ] Yes	[ ] No	[ ] Yes	[ ] No
Incident Response Plan (IRP)	[ ] Yes	[ ] No	[ ] Yes	[ ] No

Does your IRP specifically address ransomware scenarios? [ ] Yes [ ] No

OPTIONAL COVER – CRIMINAL FINANCIAL LOSS

75. Do you want cover for Criminal Financial Loss? [ ] Yes [ ] No

   Includes cyber theft, telephone phreaking, identity-based theft, push payment theft and cryptojacking.
   Does not include socially engineered theft unless selected below.

76. Aggregate limit for Criminal Financial Loss
   - [ ] $10,000 [ ] $25,000 [ ] $50,000 [ ] $75,000 [ ] $100,000 [ ] $150,000 [ ] $250,000
   - [ ] Other $

   The sublimit forms part of and is not in addition to the limit for Section B – Your Own Cyber Losses

77. Excess applicable to Criminal Financial Loss only
   - [ ] $0 [ ] $2,500 [ ] $5,000 [ ] $10,000 [ ] $15,000 [ ] $25,000 [ ] $50,000 [ ] $100,000
   - [ ] Other $

78. Do you want to include cover for socially engineered theft? [ ] Yes [ ] No

79. Sublimit for socially engineered theft

   The sublimit for socially engineered theft is included within and cannot be greater than the aggregate limit for criminal financial loss. The excess for criminal financial loss applies to socially engineered theft as well.
   - [ ] $5,000 [ ] $10,000 [ ] $15,000 [ ] $20,000 [ ] $30,000 [ ] $50,000 [ ] $75,000 [ ] $100,000
   - [ ] $125,000 [ ] $150,000 [ ] $200,000 [ ] $250,000

Continued overleaf

OPTIONAL COVER – CRIMINAL FINANCIAL LOSS (CONT.)

80. Are all new payees, and changes to existing payees' banking details, double authenticated with the payee? ☐ Yes ☐ No

81. Do transfers > $10,000 require dual signature or supervisor / manager sign off? ☐ Yes ☐ No

82. After enquiry, have you within the past 5 years suffered a crime, fidelity or computer crime loss? If Yes, please provide details: ☐ Yes ☐ No

OPTIONAL COVER – TANGIBLE PROPERTY

83. Do you want cover for Tangible Property? ☐ Yes ☐ No

The sublimit forms part of and is not in addition to the limit for Section B – Your Own Cyber Losses

OPTIONAL COVER – SYSTEM IMPROVEMENT COSTS

84. Do you want cover for System Improvement Costs? ☐ Yes ☐ No

The sublimit of $250,000 forms part of and is not in addition to the limit for Section B – Your Own Cyber Losses

OPTIONAL COVER – DIRECTORS AND OFFICERS LIABILITY (D&O)

85. Do you want cover for Directors & Officers Liability? ☐ Yes ☐ No

D&O Liability is only available for unlisted companies.

86. Aggregate sublimit for D&O Liability ☐ $250,000 ☐ $500,000 ☐ $1,000,000

The sublimit forms part of and is not in addition to the limit for Section C – Your Cyber Liability to Others.

87. Are you listed on any stock exchange, or are you planning an initial public offering or any subsequent offering during the coming 12 months? ☐ Yes ☐ No

88. Have you within the past 5 years had D&O or Management Liability (ML) insurance declined or cancelled, or are you aware, after enquiry, of any D&O or ML loss, claim, or circumstance which has or could impact you or your business or give rise to a D&O or ML claim? ☐ Yes ☐ No

If Yes, please provide details:

emergence

PRIOR CLAIMS AND CIRCUMSTANCES

89. After enquiry, within the past 5 years, are you aware of any losses, claims, circumstances, product recalls, cyber events, privacy breaches, intellectual property disputes, regulatory investigations or proceedings, crime or social engineering incidents which have impacted, or could adversely impact your business or give rise to a claim under this policy? ☐ Yes ☐ No

CLAIM 1

Total impact, including all business interruption, remediation costs and other loss? $

Date of loss: / /

Please indicate the category of the loss by ticking appropriate box:

☐ Professional Indemnity Loss ☐ Cyber Loss ☐ Public and Product Liability Loss

Please provide details of the loss/claim/circumstances/incident:

What remediation steps and controls were implemented after the loss? (Attach report if available):

CLAIM 2

Total impact, including all business interruption, remediation costs and other loss? $

Date of loss: / /

Please indicate the category of the loss by ticking appropriate box:

☐ Professional Indemnity Loss ☐ Cyber Loss ☐ Public and Product Liability Loss

Please provide details of the loss/claim/circumstances/incident:

What remediation steps and controls were implemented after the loss? (Attach report if available):

Continued overleaf

emergence

PRIOR CLAIMS AND CIRCUMSTANCES (CONT.)

CLAIM 3

Total impact, including all business interruption, remediation costs and other loss? $

Date of loss: / /

Please indicate the category of the loss by ticking appropriate box:

☐ Professional Indemnity Loss ☐ Cyber Loss ☐ Public and Product Liability Loss

Please provide details of the loss/claim/circumstances/incident:

What remediation steps and controls were implemented after the loss? (Attach report if available):

90. Have you had any unforeseen down time to your website or IT network of more than 8 hours? ☐ Yes ☐ No

If Yes, provide details including duration, how it is resolved and any cost to you:

Continued overleaf

PREFERRED LIMIT OF INSURANCE, EXCESS, AND INDEMNITY PERIOD

91. Please select your preferred Limits for each of the coverage sections below:

Professional Indemnity	Cyber	Public and Product Liability
☐ $1,000,000	☐ $250,000	☐ $5,000,000
☐ $2,000,000	☐ $500,000	☐ $10,000,000
☐ $3,000,000	☐ $1,000,000	☐ $15,000,000
☐ $4,000,000	☐ $2,000,000	☐ $20,000,000
☐ $5,000,000	☐ $3,000,000	☐ Other $
☐ $10,000,000	☐ $4,000,000	
☐ $15,000,000	☐ $5,000,000	
☐ $20,000,000	☐ $10,000,000	
☐ Other $	☐ Other $	

92. Please select your preferred excess for each of the coverage sections below:

Professional Indemnity	Cyber	Public and Product Liability
☐ $0	☐ $0	☐ $0
☐ $2,500	☐ $2,500	☐ $500
☐ $5,000	☐ $5,000	☐ $1,000
☐ $10,000	☐ $10,000	☐ $2,500
☐ $15,000	☐ $15,000	☐ $5,000
☐ $25,000	☐ $25,000	☐ $10,000
☐ $50,000	☐ $50,000	☐ $25,000
☐ Other $	☐ Other $	☐ Other $

93. Business Interruption indemnity period:

☐ 30 Days ☐ 60 Days ☐ 90 Days ☐ 180 Days ☐ 365 Days

DECLARATION

I/we acknowledge that:

1. I/we have read and understood the important information provided on the last page of this document in the important information section.
2. I/we are authorised by all those seeking insurance to make this proposal, and declare all information on this proposal and any attachment is true and correct.
3. I/we authorise the underwriter to give to, or obtain from, other insurers or any credit reference service, any information relating to insurance held by me/us or any claim in relation thereto.
4. I/we acknowledge that, where answers are provided in the proposal are not in my/our handwriting, I/we have checked and certify that the answers are true and correct.

Policyholder's signature: Date: / /

GLOSSARY

Admin/privilege service accounts

Admin/privileged accounts refer to user accounts that have elevated privileges.

Admin accounts can manage and maintain a system or network.

Privileged accounts are used for automated processes or by applications that require elevated privileges to perform a task.

AI/automated rules-based enforcement

AI/automated rules-based enforcement is a mechanism designed to enforce predefined rules within security systems. An automated rules-based system is actively monitoring and enforcing certain rules or conditions to respond to a security threat.

Application whitelisting

Application whitelisting allows only authorised and approved applications to run on a system or network.

Content control software

Content control software, commonly referred to as an Internet filter, is software that restricts or controls the content a user is able to access and/or download via the Internet.

Domain

A domain name (often called a domain) is an easy-to-remember name that's associated with a physical IP address on the Internet. It's the unique name that appears after the @ symbol in email addresses, and after www. in web addresses. Examples of domain names include google.com and wikipedia.org.

E-commerce activities

E-commerce involves the sale of goods and services over the internet. For example, online retail stores, digital products (e-books, music) and online marketplaces (eBay, Amazon etc).

Encryption

Encryption is the process of converting information or data into code to prevent unauthorised use.

Encryption at rest refers to encrypting data when it is stored on a device or storage system.

Encryption in transit refers to encrypting data as it travels across a network or between systems.

End of Life technology (EOL)

EOL refers to a stage in the life cycle of a technology product where it is no longer developed, maintained or supported by the manufacturer.

Endpoint Detection and Response (EDR)

EDR technology focuses on the detection, investigation, and mitigation of suspicious activities on endpoints including computers, servers and other devices within a network. EDR can identify anomalies and identify potential security threats.

Endpoint Protection Platform (EPP)

EPP is designed to defend endpoints such as laptops, servers and other devices connected to a network from various forms of malicious activities including malware, ransomware, and other cyber threats.

Immutable technology

Immutable technology is a type of technology or system where data or code cannot be altered or modified once it is created or deployed.

Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS)

IDS and IPS are technologies designed to detect and respond to malicious activities or security incidents within a computer network.

IDS is used to monitor a network or system and identify patterns or behaviours that may indicate unauthorised access.

IPS goes a step further than IDS by automatically blocking detected threats.

Multi-Factor Authentication (MFA)

MFA is a mechanism that requires individuals to provide more than one form of identification to access an account or system. The additional forms of identification can include one-time codes or biometrics.

Non-Fungible Token (NFT)

NFT is a digital asset such as digital content, artwork, or video that has been recorded on a blockchain to certify authenticity and ownership. NFT can be traded, sold, or licensed to others in a similar way to intellectual property rights.

Next Generation Firewall (NGFW)

NGFW combines traditional firewall capabilities with advanced functionalities such as application awareness, intrusion prevention, user identity awareness and advanced threat detection.

Operational Technology (OT)

OT is a technology that is used to monitor or control physical devices. It is typically used in an industrial setting to help manage, monitor, or control machines or processes.

Payment Card Industry (PCI) assessment

PCI assessment is a process designed to evaluate a company's handling of credit card transactions to ensure the company complies with the PCI security standards.

Programmable Logic Controller (PLC)

PLC is a system that can be programmed to do a certain task base on a pre-set instruction. It is typically used to automate industrial machinery or manufacturing processes.

Security Information and Event Management (SIEM)

A SIEM system provides real time analysis of logs that are gathered from various sources such as servers and security applications. A SIEM system will analyse the logs and identify potential security incidents.

Security patch management process

A security patch management process involves applying patches or updates to software and systems at regular intervals to address vulnerabilities and protect against security threats.

Supervisory Control and Data Acquisition (SCADA)

SCADA is a system that is used to monitor, analyse, or supervise industrial devices or processes in real-time.

emergence

It is important that you read and understand the following.

Claims made notice

Section A – Professional Indemnity and Section C – Your Cyber Liability to Others of this policy is issued on a 'claims made and notified' basis. This means that these two sections will respond to:

a. claims first made against you during the policy period and notified to us during the policy period or, if applicable, the extended reporting period (as specified in Section H - General Condition 13), provided you were not aware at any time prior to the commencement of the policy of circumstances which would have put a reasonable person in your position on notice that a claim may be made against you; and

b. facts that you may decide to notify are those which might give rise to a claim against you. Such notification must be given as soon as reasonably practicle after you become aware of the facts and prior to the expiry of the policy period. If you give written notification of facts, the policy will respond even though a claim arising from those facts is not made against you until after the policy has expired. When the policy period expires, no new notification of facts can be made to us under Section A – Professional Indemnity and Section C – Your Cyber Liability to Others.

Your duty of disclosure

When you apply for insurance, you have a legal duty of disclosure. This means you or anyone applying on your behalf must tell us everything you know (or could be reasonably expected to know) that might affect our decision when deciding:
a. to accept your insurance, and or
b. the cost or terms of the insurance, including the excess
c. In particular, you should tell us anything which may increase the chance of a claim under this policy, or the amount of a claim under this policy.

You also have this duty everytime your insurance renews and when you make any changes to it. If you or anyone on your behalf breaches this duty of disclosure, we may treat this policy as being of no effect and to have never existed.

Please ask us if you are not sure whether you need to tell us about something.

About Emergence NZ Limited

Emergence NZ Limited (NZBN: 9429051153861, FSP: 1005174) ('Emergence') acts under a binding authority given to it by the insurer to administer and issue policies, alterations and renewals. In all aspects of arranging this policy, Emergence acts as an agent for the insurer and not for you.

Contact details are:

Email: info@emergenceins.co.nz

Telephone: 0800 129 237 (0800 1 CYBER)

Postal address: Level 11, Shortland Centre, 55 Shortland Street, Auckland 1010