emergence

tech event protection

TEP-001 NZ GENERAL INFORMATION AND POLICY WORDING

tech event protection

emergence

TEP-001 NZ
General Information and Policy Wording

Contents

General Information

About Emergence NZ Limited

Emergence NZ Limited (NZBN 9429051153861) acts under a binding authority given to it by certain underwriters at Lloyd's (the underwriters) lead by Tokio Marine Kiln Syndicate 510 to administer and issue policies, alterations and renewals. In all aspects of arranging this **policy**, Emergence NZ Limited (Emergence) acts as an agent of the underwriters and not the **policyholder**.

Contact details are:

Email: info@emergenceins.co.nz

Telephone: 0800 129 237 or 0800 1 CYBER

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

About the Insurer

This insurance is underwritten by certain underwriters at Lloyd's lead by Tokio Marine Kiln Syndicate 510. If **you** require further information about this insurance or wish to confirm a transaction, please contact Emergence.

Services Available

Services available to our **Policyholders** if cover for Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others is elected.

Our Cyber Consultancy and Monitoring Service

Emergence provides a range of services to **our policyholders** when they purchase a **policy** from Emergence. These services are at no cost to the **policyholder** and are optional to the **policyholder** to take up. The services are provided in conjunction with an Emergence related company cyberSuite Pty Limited. **Policyholders** can also obtain services directly from cyberSuite that are not provided with the **policy**, at a cost to the **policyholder**.

When the **policy** is issued by Emergence it will be accompanied by a letter which sets out all the services and how **you** can access the services. The services include tips for better cyber security, an hour free consultation to discuss **your** cyber security, ongoing scanning of **your** internet-facing infrastructure to determine vulnerabilities and dark web scanning to determine if **your** data is vulnerable.

All of the services are designed to enhance **your** cyber security while **you** remain a **policyholder** with Emergence. **We** will also provide advice to **you** after a claim on how best to secure **your computer system.**

Our Cyber Breach Coach Service

If there is or **you** reasonably suspect there is a **cyber event** in **your business**, which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will provide an Emergence cyber breach coach to investigate and manage the **cyber event**. Incident response provided solely by an Emergence cyber breach coach does not form part of **cyber event response costs**, does not erode the **aggregate** and no **excess** applies to the cyber breach coach service.

HOW TO NOTIFY US IF A CLAIM IS MADE AGAINST YOU OR A CYBER EVENT HAPPENS

1. In the event **you** become aware of a **claim** made against **you**, or an incident or **occurrence** which may give rise to a **claim**, then **you** must give **us** notice in writing at **claims@emergenceins.co.nz** as soon as practicable to do so and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**.
2. In the event **you** become aware of a **cyber event, you** must immediately ring the Emergence Cyber Event Reporting Line on **0800 129 237** (that is 0800 1 CYBER) or notify Emergence in writing at **claims@emergenceins.co.nz** and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**.
3. **You** must notify **cyber theft**, **socially engineered theft, identity-based theft, push payment theft, telephone phreaking** or **cryptojacking** to, respectively, the National Cyber Security Centre, **your** financial institution, and **your** telephone service provider, within 24 hours of it first being discovered by **you**.
4. **We** will assess whether cover applies under **your policy.**
5. **You** must do everything reasonably possible to preserve evidence to enable **us** to properly assess and investigate the claim.
6. If the claim is not covered under **your policy, we** will advise **you** to engage **your** own service resources.

This is a quick reference provided for **your** convenience. Please refer to Section G of the **policy** for a full listing of Claims Conditions.

Our Agreement

Your policy is a contract of insurance between **you** and **us** and consists of the **policy wording** together with the **schedule**, and any endorsement(s) stated in **your schedule**.

How this Policy Works

Your policy is made up of several sections.

It is important to understand the type of cover **you** have purchased and how the **limits** apply. Not every financial loss is covered under the **policy**. The type of losses covered are set out in Sections A to D.

Section A – Professional Indemnity

Section B – Your Own Cyber Losses

Section C – Your Cyber Liability to Others

Section D – Public and Product Liability

Your schedule will list the cover chosen by **you** that **we** have agreed to provide. The **limit**, or sublimit, and **excess** for each cover will be stated in **your schedule.**

Section E – What Certain Words Mean

Explains the meaning of defined words used in the **policy**. These words may be used in one or more sections of the **policy**.

Section F – Exclusions

Sets out what the **policy** does not cover. These are the **policy's** exclusions.

Note: **You** should read these exclusions carefully and speak to **your** insurance broker about what this **policy** covers and what other insurance cover **you** need.

Section G – Claims Conditions

Explains what **you** must do if there is a **claim** against **you**, an incident or **occurrence** that may give rise to a **claim**, or a **cyber event.**

Section H – General Conditions

Sets out the conditions which **you** have to comply with under the **policy**.

Fair Insurance Code

We are committed to complying with the Fair Insurance Code as published by the Insurance Council of New Zealand. This means **we** will:

- provide insurance contracts which are understandable and show the legal rights and obligations of both **us** and the **policyholder;**
- explain the meaning of legal and technical words or phrases;
- explain the special meanings of particular words or phrases as they apply in the **policy**;
- manage claims quickly, fairly and transparently;
- clearly explain the reason(s) why a claim has been declined;
- provide **policyholders** with a written summary of **our** complaints procedure as soon as disputes arise and advise them how to lodge a complaint and tell them about the Insurance and Financial Services Ombudsman Scheme;

If the claim is not covered under **your policy**, **we** will advise **you** to engage **your** own service resources. **We** will clearly explain the reasons why a claim is denied.

Any word in **bold** in General Information has the same meaning as given to it in the **policy**.

Policy Wording

What This Policy Covers

This **policy wording** and **your schedule**, which includes any endorsement(s), determines the cover **we** provide to **you** under this **policy**. It is important that **you** read and understand the **policy** in its entirety.

Each Section, each Extension and each Optional Cover under this **policy** is subject to a **limit** or a sublimit.

The **limit** and the **aggregate** under Section A – Professional Indemnity of the **policy** is stated in the **schedule**. Each Extension under Section A – Professional Indemnity is subject to a sublimit which is stated in the **schedule**. Each sublimit for each Extension is the most **we** will pay under that extension and forms part of the **aggregate** for Section A – Professional Indemnity.

The **limit** under Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others of the **policy** is stated in the **schedule**. There is one **aggregate** for both Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others of the **policy** which is stated in the **schedule**. All Extensions and Optional Covers under Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others are subject to a sublimit which is stated in the **schedule**. Each sublimit for each Extension or Optional Cover is the most **we** will pay under that Extension or Optional Cover and forms part of the **aggregate** for Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others.

The **aggregate** for Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others form part of and is included in the **aggregate** for Section A - Professional Indemnity.

The **limit** and the **aggregate** under Section D - Public and Product Liability of the **policy** is stated in the **schedule.** Each Extension under Section D - Public and Product Liability is subject to a sublimit which is stated in the **schedule**. Each sublimit for each Extension is the most **we** will pay under that extension and forms part of the **aggregate** for Section D - Public and Product Liability.

The **limit** stated in your **schedule** is exclusive of GST.

Section A – Professional Indemnity

We will pay a **loss** that **you** are legally liable for arising out of a **claim** first made against **you** and notified to **us** during the **policy period**, caused by actual or alleged:

a. **technology wrongful act,**
b. **intellectual property wrongful act,**
c. **media wrongful act,**

committed by **you** or on **your** behalf which happened on or after the **retroactive date** and within the **territorial limits** during the course of **you** providing **professional services** or **products**.

Extensions to Section A – Professional Indemnity

The following extensions apply to Section A – Professional Indemnity only and do not extend to any other section of the **policy**. The extensions apply to **claims** first made and notified to **us** during the **policy period** arising out of actual or alleged **technology wrongful act**, **intellectual property wrongful act**, or **media wrongful act**, committed by **you** or on **your** behalf which happened on or after the **retroactive date** and within the **territorial limits** during the course of **you** providing **professional services** or **products**.

Extension A1 – Dishonesty or Fraudulent Act of Another Insured

We will pay a **loss** from a **claim** that **you** are legally liable for arising out of an actual or alleged dishonest or fraudulent act or omission by another **insured** provided such act or omission is committed (or alleged to have been committed) without **your** knowledge and is not approved or instructed by **you**.

We will also pay for **your** own losses, including reasonable and necessary costs or expenses, that **you** incur as a direct result of such dishonest or fraudulent act or omission.

We will provide cover for the innocent **insured(s)** only and no cover will be available to the **insured(s)** committing the dishonest or fraudulent act or omission.

Under this extension, **we** will not waive **our** rights of recovery against the person or entity who committed the dishonest or fraudulent act or omission, and **you** must do everything reasonably possible to assist **us** in **our** attempt to make a recovery.

Extension A2 – Mitigation Costs or Expenses

We will pay **you** for mitigation costs or expenses that **you** incur with **our** prior **consent**, solely for the purpose of mitigating or avoiding an actual or potential **claim** against **you**.

Extension A3 – Mitigation of Unpaid Fees

We will pay **you** any unpaid **professional service** fees or **product** costs **you** have invoiced to **your** customer provided that:

a. the customer's refusal to pay is related to actual or alleged deficiencies of **your product** or **professional service**; and
b. that continuing to pursue such fees or costs would likely cause a retaliatory action including a **claim** against **you**.

In the event that a **claim** is ultimately made against **you**, any payment under this extension will be deducted from any later indemnity payments that **you** may otherwise be entitled to under this **policy**.

Extension A4 – Refund of Fees

We will pay a **loss** from a **claim** for any refund of **professional services** fees or **product** costs that **you** are legally liable to return to customers, except for the part of the fees or costs that represent **your** profit margin and/or any tax component.

Extension A5 – Vicarious Liability

We will pay a **loss** from a **claim** that **you** are legally liable for, arising out of **products** or **professional services** supplied to third parties on **your** behalf by **your IT contractor**.

Extension A6 – Intellectual Property Pursuit Costs

We will pay for **intellectual property pursuit costs** that **you** incur as a direct result of enforcing or pursuing a third party for breach of **your** intellectual property rights, that **you** become aware of and notify to **us** during the **policy period**, whether actual or suspected, within the **territorial limits** and subject always to **good prospects of success.**

This extension does not apply to any **intellectual property pursuit costs** within the jurisdiction of the United States of America, their territories or possessions.

Section B – Your Own Cyber Losses

Section B1 – Business Interruption

This section is subject to waiting periods.

a. If a **cyber event** or **system failure** happens at or within **your business** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** the **impact on business costs**. The maximum **we** will pay in any one **policy period** for **system failure** under Section B – Your Own Cyber Losses is the sublimit stated in the **schedule**.

b. If a **cyber event** or **system failure** happens at or within **your IT supplier's business**, which is first discovered by **you** and notified to **us** during the **policy period** then **we** will pay **you** the **impact on business costs**. The maximum **we** will pay in any one **policy period** for **system failure** under Section B – Your Own Cyber Losses is the sublimit stated in the **schedule**.

c. If a **preventative shutdown** first happens during the **policy period** which is notified to **us** during the **policy period**, then **we** will pay **you** a **preventative shutdown allowance**. The **preventative shutdown allowance** is the maximum **we** will pay in any one **policy period** for all **preventative shutdowns** and is the sublimit stated in **your schedule**. The sublimit is included in and forms part of the **limit** for Section B – Your Own Cyber Losses.

Section B2 – Cyber Event Response Costs

a. If there is a **cyber event** at or within **your business**, or **you** reasonably suspect there is a **cyber event** at or within **your business**, which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay or reimburse **your cyber event response costs**.

b. If there is a **cyber event** at or within **your IT supplier's business** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **your IT supplier response costs**.

Optional Cover under Section B of the Policy

Section B3 – Criminal Financial Loss Cover

We will pay a **direct financial loss** to **you**, a **direct financial loss** to others, and any i**nvestigation costs** directly arising out of:

a. **cyber theft**;

b. **socially engineered theft**;

c. **identity-based theft**;

d. **push payment theft**;

e. **telephone phreaking**; or

f. **cryptojacking**

provided that the events in a. to f. are first discovered by **you** and notified to **us** during the **policy period.**

We will also pay **pursuit costs** of up to a maximum of $50,000 paid with **our** prior **consent** to a third party (other than a law enforcement officer or **your** current or former employee or **IT contractor**), as reward for assistance leading to the arrest and conviction of the threat actor of a **cyber theft**, **socially engineered theft**, **identity-based theft**, **push payment theft**, **telephone phreaking** or **cryptojacking**.

Section B4 – Tangible Property Cover

We will pay the cost of the replacement or repair of **your computer system** hardware at or within **your business** that is physically damaged or no longer suitable for use solely and directly due to or resulting from a **cyber event** covered under this **policy** or the incurring of related **cyber event response costs**.

Section B5 – System Improvement Costs

We will reimburse reasonable and necessary costs, up to the sublimit shown on **your schedule**, that **you** incur with **our** prior **consent**, to replace or restore **your computer system** software that is no longer suitable for use with an upgraded or improved version following a **cyber event** that is covered under this **policy**.

Section C – Your Cyber Liability to Others

We will pay a **loss** that **you** are legally liable for arising out of a **claim** that is first made against **you** and notified to **us** during the **policy period**, because of an actual or alleged:

1. **cyber event**, except for **cyber wrongful act,** or
2. **Payment Card Industry liability**

at or within **your business** which took place on or after the **retroactive date** and within the **territorial limits**.

Extensions to Section C – Your Cyber Liability to Others

The following extensions apply to Section C – Your Cyber Liability to Others only and do not extend to any other section of the **policy**.

Extension C1 – Mitigation Costs or Expenses

If a **cyber event** happens at or within **your business** or **your IT supplier's business** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** for mitigation costs or expenses **you** incur with **our** prior **consent**, solely for the purpose of mitigating or avoiding an actual or potential **claim** against **you**.

Optional Cover under Section C of the Policy

Section C2 – Directors & Officers

We will pay a **loss** that any of **your** directors or officers is legally liable for arising out of a **claim** that is first made against **your** directors or officers and notified to **us** during the **policy period** because of a **D&O cyber wrongful act** in **your business**.

This Optional Cover will not apply to the following:

a. If **you** are listed on the New Zealand Stock Exchange, if **your** shares are traded on any other exchange, or if **you** are pursuing any actual or proposed initial or subsequent public offering.

b. Any **claim** arising out of, or made in the United States of America, its territories or possessions, or by, or on behalf of, **you** or any director or officer.

Section D – Public and Product Liability

We will pay a **loss** arising out of an **occurrence** that **you** are legally liable for in the course of **your business**, including liability **you** have assumed under contract, caused by actual or alleged:

a. **personal injury**,

b. **property damage**,

c. **pollution** – except for **pollution** or a **claim** occurring in the United States of America, their territories and possessions,

that happen during the **policy period** and within the **territorial limit**.

Extensions to Section D – Public and Product Liability

The following extensions apply to Section D - Public and Product Liability only and do not extend to any other section of the **policy**.

Extension D1 – Product Recall Expenses

We will pay **product recall expenses** incurred by **you** due to a necessary **product** recall because **you** have discovered the use or consumption of any such **product** has resulted, or is reasonably expected to result in, **personal injury** or **property damage**.

Extension D2 – Care, Custody, or Control

We will pay a **loss** from a **claim** that **you** are legally liable for, arising out of a loss of property or **property damage** to any property of a third party, that is under **your** care, custody, or control.

This extension also applies to **property damage** to a visitor's or an employee's vehicle, including the loss of contents and accessories from the vehicle, that is in a car park owned or operated by **you** provided that:

a. The vehicle is not owned by, or used in conducting, **your business.**

b. The car park is not operated by **you** for income as car park operator.

Extension D3 – Key Person Loss

We will pay reasonable and necessary costs **you** incur with **our** prior **consent**, for the purpose of managing public communications following a **personal injury** suffered by any of **your** principals, partners, directors or officers.

Section E – What Certain Words Mean

The words listed below have been given a specific meaning in this **policy** and these specific meanings apply when the words appear in **bold** font.

1. **act(s) of cyber terrorism** means the premeditated use of disruptive activities against **your computer system** or a **computer system** operated by **you**, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity, in each case with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives. **Act(s) of cyber terrorism** does not include any such activities which are:
   a. part of or in support of any use of military force;
   b. at the direction of, or under the control of a government or sovereign state;
   c. a **cyber operation**;
   d. a **war**.

2. **act(s) of terrorism** means a premeditated use of disruptive activities, or the explicit threat to use such activities, by an individual or group of individuals, whether acting alone or on behalf of or in connection with any entity or government, with the intention to cause harm, further social, ideological, religious, political or similar objectives, or to intimidate any person(s) in furtherance of such objectives.

3. **aggregate** means:
   a. Under Section A – Professional Indemnity – the maximum **we** will pay under Section A – Professional Indemnity in any one **policy period** for all **insureds**.
   b. Under Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others – the maximum **we** will pay in any one **policy period** for all **insureds**. Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others share the same **aggregate** and the **aggregate** for Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others forms part of the **aggregate** for Section A – Professional Indemnity.
   c. Under Section D - Public and Product Liability - the maximum **we** will pay under Section D - Public and Product Liability in any one **policy period** for **loss** caused by (a) **personal injury** and/or **property damage** resulting from **products** (shown as product liability in **your schedule**) and (b) **pollution** for all **insureds**, but (c) **loss** caused by **personal injury** and/or **property damage** not resulting from **products** (shown as public liability in **your schedule**) are subject to a **limit** per **occurrence**.
4. **business** means:
   a. any commercial activities conducted by **you** or on **your** behalf, or
   b. any supporting activities necessary for the conduct of **your business**, or
   c. any activities or events organised by **you** for **your** employees or customers for the conduct of **your business**.
5. **claim(s)** means any written demand, notice of pending action or civil, criminal, administrative, regulatory, mediatory or arbitral proceedings against **you** seeking monetary or non-monetary relief.
6. **computer system** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, systems, firmware, networks, platforms, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility leased, owned, or operated by **you** or on **your** behalf.

   In respect of Exclusion 7 War and Cyber Operation and the associated definition of **cyber operation** only, **computer system** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility.
7. **consent** means **our** consent, which will not be unreasonably withheld.
8. **cryptojacking** means the unauthorised use of **your computer system** to mine digital currency that causes **you direct financial loss.**
9. **cyber event** means any of the following:
   a. **crimeware** which means any type of unauthorised code intentionally designed to damage, alter, or extract data or information from a **computer system** including any type of malicious, corrupting or harmful software, malware, computer virus, Trojan horse, brickerbots, wiperware, botware, crimeware keystroke logger, spyware, adware, worm, ransomware, scareware, rogueware, malicious trap door, ransomworm, rootkit, malicious active content, logic bomb or advanced persistent threat (or equivalent) but does not include **cyber espionage** or **point of sale intrusion**.
   b. **cyber espionage** which means unauthorised access to an item of a **computer system** linked to a state affiliated or criminal source exhibiting the motive of espionage.
   c. **cyber extortion** which means a credible threat or series of credible threats involving ransomware that includes a demand for money or other valuable consideration (including digital currency) to avert or stop the threat of a **cyber event**.
   d. **denial of service** which means an unauthorised interference or malicious attack that restricts or prevents access to **your computer system** for person(s) or entities authorised to gain access. This includes a distributed **denial of service**.
   e. **hacking** which means malicious or unauthorised access to a **computer system**.
   f. **insider and privilege misuse** which means unapproved or malicious use of a **computer system** by **your** employees, outsiders in collusion with **your** employees, or business partners who are granted privileged access to a **computer system** but does not include theft, **socially engineered theft**, **identity-based theft**, **push payment theft** or **cyber theft**.
   g. **miscellaneous errors** which means unintentional actions directly compromise a security attribute of an item of a **computer system** but does not include theft, **socially engineered theft** or **cyber theft**.
   h. **payment card skimming** which means a skimming device being physically implanted through tampering into an item of a **computer system** that reads data from a payment card.
   i. **physical theft and loss** which means that an item of a **computer system** is missing or falls into the hands of a third party or the public whether through misplacement or malice.
   j. **point of sale intrusion** which means a remote attack against a **computer system** where retail transactions are conducted, specifically where purchases are made by a payment card.

k. **privacy error** which means acts or omissions by **your** employees that lead to unauthorised access to, unauthorised disclosure of or loss of data (including non-electronic data) which necessitates incurring **notification costs**, **data and system restoration costs**, or **identity theft response costs**.

l. **web app attacks** which means that a web application was the target of attack against a **computer system**, including exploits of code level vulnerabilities in the application.

10. **cyber event response costs** means the reasonable and necessary costs and expenses **you** incur with **our consent**, being:

    a. **credit and identity monitoring costs** which means costs incurred in engaging monitoring services by a third party for persons affected by a **cyber event** for a period of up to twelve (12) months;

    b. **cyber extortion costs** which means costs paid by **you** to respond to a **cyber event** as a direct result of **cyber extortion**. Any **cyber extortion costs** will be deemed for the purposes of this **policy** to be insurable unless there is case law, legislation, regulation or an order or judgement from a regulator, legislator or law enforcement agency specifically prohibiting the insurability of the **cyber extortion costs**. If insurable, and upon presentation of evidence of payment, then **we** will reimburse the **cyber extortion costs** paid by **you**;

    c. **data and system restoration costs** which means costs incurred in restoring or replacing **your** data, data **you** hold or process on behalf of others, programs (or software or applications) in **computer system** that have been lost, damaged or destroyed and the cost to mitigate or prevent further damage, and includes the cost of **you** purchasing replacement licenses, if necessary, but does not include any costs relating to redesign, replication or reconstitution of proprietary information, facts, concepts or designs;

    d. **data securing costs** which means costs incurred in securing a **computer system** to avoid ongoing **impact on business costs**, **loss** and **cyber event response costs**;

    e. **external management costs** which means costs incurred in responding to a **cyber event** including crisis management and mitigation measures engaged in by **you** and agreed to by **us** when necessary to counter a credible impending threat to stage a **cyber event** against **computer system** and to prevent reputational harm to **you**;

    f. **identity theft response costs** which means costs incurred in supporting an individual with reporting of the **identity theft** and re-establishing identity and essential records following the **identity theft**;

    g. **IT forensic costs** which means costs incurred by **you** with **our** prior **consent**, to investigate a **cyber event** or suspected **cyber event**;

    h. **legal advice costs** which means costs incurred with **our** written **consent** to advise **you** in the response to a **cyber event**. **Legal advice costs** do not include **defence costs**;

    i. **notification costs** which means costs incurred in notifying any person whose data or information has been accessed or lost including the cost of notifying a privacy breach to the Office of the Privacy Commissioner or other authorities;

    j. **public relations costs** which means costs incurred in responding to a **cyber event**, or adverse media arising from a **cyber event**, including external public relations, media, social media and communications management to prevent reputational harm to **you**;

    k. **pursuit costs** which means costs of up to a maximum of AUD 50,000 paid with **our** prior **consent** to a third party (other than a law enforcement officer or **your** current or former employee or **IT contractor**), as reward for assistance leading to the arrest and conviction of the threat actor of a **cyber event** covered under this **policy**; and

    l. **virus extraction costs** which means costs incurred to remove a virus from **computer system**.

11. **cyber operation** means the use of a **computer system** by, at the direction of, or under the control of a sovereign state to:

    a. disrupt, deny access to or degrade functionality of a **computer system**; and/or

    b. copy, remove, manipulate, deny access to or destroy information in a **computer system**.

12. **cyber theft** means an electronic transfer of funds, accounts receivable or securities that results in **direct financial loss**. The **cyber theft** must happen directly because of a **cyber event** that happens to **your computer system** and without **your** knowledge. **Cyber theft** does not include **push payment theft**, **socially engineered theft** or **identity-based theft**.

13. **cyber wrongful act** means **insider and privilege misuse**, **miscellaneous errors**, and **privacy error**.

14. **D&O cyber wrongful act** means an act, error, omission, breach of duty, or neglect directly arising out of a covered **cyber event** that leads to the personal liability of any of **your** directors or officers that is not otherwise insured and that **you** do not otherwise indemnify.

15. **defence costs** means the reasonable costs, charges, fees and expenses incurred with **our** prior written **consent** to defend, investigate, appeal or settle a **claim**. **Defence costs** do not include **legal advice costs**.

16. **delayed revenue** means **revenue** earned in the period of ninety (90) calendar days after the end of the **indemnity period** which would have been earned during the **indemnity period** if the **cyber event** or **system failure** did not happen.

17. **direct financial loss** means:
    a. **your** funds, accounts receivable or securities, or the funds, accounts receivable or securities in **your** control belonging to others, that are lost due to **cyber theft**, **identity-based theft** or **socially engineered theft** and remain unrecoverable, or
    b. **your** customers funds that are lost due to **push payment theft** and remain unrecoverable, or
    c. unintended or unauthorised call charges or bandwidth charges in excess of normal and usual amounts that **you** must pay caused by **telephone phreaking**, or
    d. unintended or unauthorised bandwidth charges, electricity costs, or cloud usage charges in excess of normal and usual amounts that **you** must pay caused by **cryptojacking**.

    direct financial loss does not include digital or crypto currencies, gift cards, vouchers, coupons or reward points.

18. **employment wrongful act** means any actual or alleged employment-related act, error, omission or conduct constituting actual, constructive or alleged: wrongful dismissal, discharge or termination of employment; wrongful failure to employ or promote; wrongful deprivation of career opportunity; misleading representation or advertising in respect of employment; wrongful disciplinary action; negligent employee evaluation; wrongful demotion; breach of employment contract; sexual or workplace harassment (including the creation of a workplace environment conducive to such harassment); wrongful discrimination; failure to grant tenure; invasion of privacy or defamation. **Employment wrongful act** does not mean employee data impacted by a **cyber event.**

19. **essential service** means a service that is essential for the maintenance of vital functions of a sovereign state including but not limited to, financial institutions and associated financial market infrastructure, health services or utility services.

20. **excess** means the amount of money that **you** are responsible for before **we** make a payment under the **policy**. The **excess** is set out in **your schedule** and is exclusive of GST. If there is more than one **excess** stated in **your schedule**, then **you** will pay the higher **excess** if the incident, claim, **occurrence**, recall, pursuit, or key person loss relates to that higher **excess**.

21. **good prospects of success** mean based on the advice of a qualified independent expert appointed by **you** with **our** prior agreement that:
    a. **you** are more likely than not to succeed on all principal points of the proposed enforcement of **your** intellectual property rights against a third party;
    b. **you** have accounted for the likely potential response of the opposing party in the overall prospect of success, including an assessment of the ability of **your** intellectual property rights to withstand legal challenge; and
    c. the reasonably expected financial benefit of the proposed enforcement of **your** intellectual property rights exceeds the expected **intellectual property pursuit costs** that will be incurred.

    The cost of obtaining advice to this effect will be reimbursed by **us** if **good prospects of success** are evidenced to **our** satisfaction, subject to the applicable sublimit.

22. **identity theft** means the unauthorised use of the identity of an individual whose data or information has been accessed because of a **cyber event** that happens to **your computer system**. **Identity theft** does not include **identity-based theft**.

23. **identity-based theft** means an **identity theft** that happens without the individual's knowledge and results in **direct financial loss** to the individual. **Identity-based theft** does not include **cyber theft**, **push payment theft** or **socially engineered theft**.

24. **impact on business costs** means:
    a. the amount that the **revenue you** earn during the **indemnity period** falls short of the **revenue you** ordinarily earn directly as a result of a **cyber event** or **system failure**, less any consequent savings, and less any **delayed revenue**, plus
    b. the net increased costs incurred by **you** during the **indemnity period** to avoid a reduction in **revenue** directly as a result of a **cyber event** or **system failure** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **revenue** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries or overhead expenses.

    Impact on business costs do not include **cyber event response costs.**

    The amount is calculated by reference to the **records of your business** and any other documents that **we** reasonably request. **We** will not pay **impact on business costs** incurred during the waiting period after **you** discover a **cyber event** or first interruption to **your business** due to a **system failure**. The waiting periods for **cyber event** and **system failure** are stated on **your schedule** and may be different.

25. **impacted state** means any sovereign state where a cyber operation has had a major detrimental impact on:
    a. the functioning of that sovereign state due to disruption to the availability, integrity or delivery of an **essential service** in that sovereign state; and/or
    b. the security or defense of that sovereign state.

26. **indemnity period** means the period starting from first discovery of the **cyber event** or **system failure** until the **computer system** is restored to its usual function, plus reasonable additional time to allow for **your business** to normalise, however in total length not exceeding the number of days set out in **your schedule**.

27. **intellectual property pursuit costs** mean the reasonable and necessary costs, charges, fees and expenses incurred with **our** prior written **consent** to investigate, prosecute or settle an enforcement action.

28. **intellectual property wrongful act** means any infringement, misappropriation, passing off, plagiarism or piracy of ideas or intellectual property rights, including copyright, trademark, registered design, circuit layout rights, domain name, service mark, slogan, metatags, trade name, trade secrets, and patent rights.

29. **investigation costs** mean costs **you** incur with **our** prior **consent**, to investigate and substantiate the circumstances and amount of a **socially engineered theft**.

30. **IT contractor** means an individual consultant or a business **you** do not own, operate or control, but that **you** engage under contract to provide **professional services** or **products** to others on **your** behalf.

31. **IT supplier** means a business **you** do not own, operate or control, but that **you** hire under contract to provide, maintain, service, process data, or manage information technology services to **you** that are used in **your business**.

32. **IT supplier response costs** mean the reasonable and necessary costs and expenses **you** incur in responding to a **cyber event** at or within **your IT supplier's business** that impacts **your** data, being:
    a. **credit and identity monitoring costs,**
    b. **cyber extortion costs**,
    c. **data and system restoration costs**,
    d. **data securing costs,**
    e. **external management costs,**
    f. **identity theft response costs,**
    g. **legal advice costs,**
    h. **notification costs,** and
    i. **public relations costs.**

    IT supplier response costs does not mean the **IT supplier's** own costs.

33. **limit** means the amount set out in the **schedule** for each of Section A – Professional Indemnity, Section B – Your Own Cyber Losses, Section C – Your Cyber Liability to Others, and Section D – Public and Product Liability of **your policy**, irrespective of the number of claim(s). The **limit** or sublimit for any Extension or Optional Cover is also set out in **your schedule**.

34. **liquidated damages** mean a specified amount of monetary penalty or service credit **you** are liable to pay arising out of liquidated damages clauses, penalty clauses, or performance warranty clauses within a contract. The **liquidated damages** specified in the contract must be fair and reasonable estimates that could be recovered against **you** in a common law claim had liquidated damages not been specified in the contract.

35. **loss** means:
    a. any sums payable pursuant to judgements (including orders for costs), settlements, awards and determinations, including damages,
    b. claimant's legal costs,
    c. regulatory and civil fines and penalties in respect of a **claim**, and such amounts will be deemed to be insurable unless there is case law, legislation, regulation or an order or judgement from a regulator, legislator or law enforcement agency prohibiting the insurability of these items,
    d. any costs as consequence of a mandatory notice from a regulatory authority as a consequence of the failure to secure information held by **you**,
    e. necessary and reasonable costs of regulatory or government inquiries,
    f. necessary and reasonable court attendance costs up to $250,000, directly related to **our** request for **you** to attend any court or other legal procedure to assist in the investigation or defence of any **claim** under this **policy**. The **excess** does not apply to court attendance cost,
    g. **defence costs**,
    h. For Section A – Professional Indemnity, **loss** includes **liquidated damages** arising from breach of contract; and **cyber event response costs** of a third party **you** become legally liable to pay under a contract,
    i. For Section A – Professional Indemnity and Section C – Your Cyber Liability to Others, **loss** also includes any aggravated, punitive, or exemplary damages, and such amounts will be deemed to be insurable unless there is case law, legislation, regulation or an order or judgement from a regulator, legislator or law enforcement agency prohibiting the insurability of these items,
    j. For Section D – Public and Product Liability, **loss** also includes costs of administering first aid up to $10,000, following an **occurrence** which leads to **personal injury**. The **excess** does not apply to cost of administering first aid.

36. **media wrongful act** means any:
    a. breach of confidentiality, breach of privacy and misuse of confidential information,
    b. libel, slander, misstatement, misrepresentation, defamation (but not any employment-related defamation, which will be deemed an **employment wrongful act**), and product disparagement,
    c. improper deep linking, framing, or web harvesting.

37. **occurrence** means an event or series of events attributable to one original source or cause that is neither expected nor intended from the viewpoint of the **insured**, regardless of whether it occurs at the same time or at the same location.

38. **Payment Card Industry liability** means the fines, penalties and monetary assessments that **you** are legally liable to pay as a direct result of **your** non-compliance with a Payment Card Industry Data Security Standard. **Payment Card Industry liability** does not mean any fine or penalty for any continuous or related or repeated non-compliance after the initial monetary fine or assessment.

39. **personal injury** means physical and mental injury sustained by a person due to an **occurrence**, including death, sickness, illness, disease, and where resulting from physical injury, emotional distress, mental anguish, humiliation, psychological harm, false arrest, false detention, false imprisonment, malicious prosecution, wrongful entry, wrongful eviction.

40. **policy** means this **policy wording**, the **schedule** and any endorsement(s) stated in **your schedule**.

41. **policy period** means the period set out in **your schedule**.

42. **policy wording** means this document.

43. **policyholder** means the entity first named in **your schedule** under **Policyholder** and is authorised to enter into and deal with this **policy** on behalf of all other entities covered under the **policy**. **Policyholder** must be domiciled in or operate from New Zealand.

44. **pollution** means the sudden, accidental and identifiable discharge, dispersal, seepage, migration, release or escape of smoke, vapours, soot, fumes, acids, alkalis, toxic, chemicals, liquids or gases, waste materials (including recycled, reconditioned, or reclaimed materials), or other irritants, contaminants, or pollutants into or upon the atmosphere, land (including building(s) or other structures thereon) or any water course or body of water.

45. **preparation costs** mean the costs **we** will pay to assist **you** to verify i**mpact on business costs** incurred by **you**.

46. **preventative shutdown** means the reasonable, necessary and intentional shut down of **your computer system** in response to a **cyber event** at or within **your business**, or a credible threat to **your computer system** following:

    a. a **cyber event** at or within **your** direct customer, **IT supplier** or business partner's business,

    b. specific instruction from **your** financial institution, law enforcement or the National Cyber Security Centre (NCSC), CERT NZ or similar agency of the government, or

    c. communication by a third party threatening to carry out **cyber extortion**, a **denial of service** attack or other **cyber event** against **your business**,

    where the events in a. to c. are first discovered by **you** during the **policy period** and where such shutdown will mitigate the threat or avoid otherwise larger claims under this **policy**.

    Preventative shutdown does not include shutdown due to routine maintenance, patching or updating of software, use of software that is past its end-of-life and no longer supported or for any reason other than mitigation of threat to **your computer system**.

47. **preventative shutdown allowance** means:

    a. the amount that the **revenue you** earn during the **preventative shutdown** falls short of the **revenue you** ordinarily earn directly as a result of the **preventative shutdown**, less any consequent savings and less any **delayed revenue**, plus

    b. the net increased costs incurred by **you** to avoid a reduction in revenue directly as a result of a **preventative shutdown** provided the amount of increased costs paid is less than **we** would have paid for a reduction in standard **revenue** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries or overhead expenses.

    c. Reasonable and necessary costs **we** agree to for an independent security audit to assess the threat to **computer system**.

    preventative shutdown allowance does not include **cyber event response costs**, **IT supplier response costs**, or **impact on business costs**. **Preventative shutdown allowance** does not include the cost for **you** to implement critical security audit recommendations or other measures as required to mitigate the threat.

    The amount is calculated by reference to the **records of your business** and any other documents that **we** reasonably request. **We** will not pay **preventative shutdown allowance** during the waiting period of the first 8 hours after **you** initiate a **preventative shutdown** unless a different waiting period has been specified on **your schedule**. The **excess** does not apply to the **preventative shutdown allowance**. **We** will pay a **preventative shutdown allowance** for up to a maximum of 48 consecutive hours after the waiting period and ending at the earlier of:

    a. first discovery of the **cyber event** affecting **your computer system**; or

    b. the safe resumption of operations of **your computer system**; or

    c. the expiration of the 48 consecutive hours.

48. **product** means any goods or products which are manufactured, produced, developed, constructed, erected, installed, repaired, maintained, sold, supplied, or distributed by **you** or on **your** behalf in connection with **your business**.

49. **product recall expenses** mean reasonable and necessary expenses incurred by **you** due to a recall of a **product** for:

    a. any communication, broadcasting, media announcements of the recall,

    b. transporting the recalled **products** from any distributor, retailer, purchaser, or user to a location designated by **you**,

c. rental of temporary housing, warehouse or storage to store the recalled **products**,

d. properly disposing of the recalled **products** and packaging that cannot be reused,

e. additional remuneration paid to **your** employees for overtime or additional employees **you** hire to cope with the recall of **products**,

f. necessary accommodation, transportation, or additional expenses of **your** employees in connection with the recall,

g. any public relations or crisis response communication in relation to the recall.

50. **professional service** means any services performed in connection with **your business**.

51. **property damage** means physical damage to, destruction of, loss of, or loss of use of tangible property due to an **occurrence**. **Property damage** does not mean physical damage to, destruction of, loss of, or loss of use of a document or data.

52. **push payment theft** means the fraudulent issuance of an invoice from **your computer system** by an unknown party that causes **your** customer **direct financial loss**. The **push payment theft** must happen directly because of a **cyber event** that happens at or within **your business** and without **your** knowledge. **Push payment theft** does not include **cyber theft**, **socially engineered theft** or **identity-based theft**.

53. **records of your business** mean all documents that evidence **your revenue**, including **your** bank records, GST records, tax records and usual business records including records that evidence **your** expenditure and outgoings.

54. **retroactive date** means the retroactive date specified in the **schedule**.

55. **revenue** means the money paid or payable to **you** for goods sold, work performed, and services rendered in the course of **your business**.

56. **schedule** means the document **we** provide to **you** which sets out the personalised details of **your policy** with **us**.

57. **socially engineered theft** means an electronic transfer of funds, accounts receivable or securities to an unintended third party that results in **direct financial loss**. The transfer must be made in connection with **your business** by **your** employee in good faith, in reliance upon intentionally misleading material facts communicated through **your computer system**, having believed such facts to be genuine and true.

    Socially engineered theft does not include **cyber theft**, **push payment theft** or **identity-based theft**.

58. **subsidiary** means an entity other than the **policyholder** or joint venture or consortium, in which, at the inception of this **policy**, **you** have majority ownership, control the composition of the board of directors, or control greater than 50% of the voting rights. **Subsidiary** includes entities **you** form or acquire during the **policy period** that also meet the following criteria, but only for **claims** or **cyber events** that happen after the date of such formation or acquisition:

    a. the **business** activity is the same as or substantially similar to **your business** activity;

    b. the entity's **revenue** does not exceed 25% of the **revenue** declared under this **policy**;

    c. the entity is not domiciled or incorporated or listed in the United States of America, or has or holds or processes data for clients or direct customers located there;

    d. the entity has not had any **claims**, losses, or **cyber events**, prior to **you** acquiring it;

    e. the entity's **computer system** and risk management are equal to or better than **yours**, or **you** will use best endeavours either to bring its **computer system** and risk management to an equivalent standard or to ensure its **computer system** will be absorbed promptly into **your computer system**.

    If a new **subsidiary** falls outside of criteria a. or b. above, automatic cover will be provided for a period of sixty (60) calendar days from the date of such formation or acquisition. **We** may extend this automatic cover beyond the sixty (60) calendar days with prior written agreement from **us** and where **you** agree to the terms of any such extension of coverage.

59. **system failure** means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **computer system**, but does not include outage:

    a. caused by a **cyber event**;

    b. caused by using untested, disapproved or illegal software, or software that is past its end-of-life and no longer supported;

    c. caused by use of a non-operational part of **computer system**;

    d. falling within parameters of a service level agreement;

    e. arising out of commercial dispute, failure to pay for services or refusal to deliver services paid for.

    The waiting period for **system failure** is stated in **your schedule**.

60. **technology wrongful act** means any:
    a. act, error or omissions,
    b. breach of professional duty,
    c. failure of **your products** or **professional services**,
    d. breach of contractual obligations - including liability **you** have assumed under contract,
    e. breach of Consumer Guarantees Act 1993 as well as any similar legislation and any amendments thereof,
    f. loss of, or damage to documents or data of others,
    g. **cyber wrongful act**,
    h. any other civil liability not mentioned above.
61. **telephone phreaking** means **hacking** of **your business** telephone systems that causes **you direct financial loss**.
62. **territorial limit** means the territorial limit specified in the **schedule**.
63. **utility provider** includes providers of gas, electricity, water, sewage, stock exchanges, security exchanges, telecommunications, satellite, cable, internet access, internet backbone, Domain Name Systems (DNS) servers or other core infrastructure of the internet.
64. **war** means armed conflict involving physical force:
    a. by a sovereign state against another sovereign state, or
    b. as part of a civil war, rebellion, revolution, insurrection, military action or usurpation of power,

    whether war be declared or not.
65. **we/our/us** means certain underwriters at Lloyd's led by Tokio Marine Kiln, Syndicate 510 (the underwriters), as insurers of this **policy** and Emergence acting on behalf of underwriters as the issuer of this **policy**.

    Note: **You** can obtain further details of the underwriters from Emergence upon request.
66. **you/your/insured** means:
    a. the **policyholder** referred to in **your schedule**,
    b. **policyholder's subsidiaries**,
    c. any affiliates stated in **your schedule**,
    d. any current, future or former employee for work performed in connection with **your business**, including directors and officers, or partners if **you** are a partnership,
    e. In the event of **your** death, incompetence or bankruptcy, if **you** are a natural person, it also includes **your** estate, heirs, legal representatives or assigns for **your** legal liabilities,
    f. any natural person **you** engage, with or without a contract, to perform any service in connection with **your business**,
    g. with respect to Section A – Professional Indemnity, Section C – Your Cyber Liability to Others, and Section D - Public and Product Liability only:
        i. **IT Contractors** under a written contract with the **policyholder** and/or the **policyholder's subsidiaries** and while acting under the instructions of the **policyholder** and/or the **policyholder's subsidiaries**,
        ii. **your** participation in any joint venture or consortium, save that no other third-party participants in such joint venture or consortium will be deemed as an **insured**.
    h. With respect to Section D - Public and Product Liability only:
        i. persons or organisations that lease premises or equipment to **you** under a written contract, or
        ii. vendors that distribute **your product** under a written contract with **you**, or
        iii. persons or organisations that **you** are obligated to insure pursuant to a written contract.

Section F – Exclusions

Exclusions – All Policy Sections

The following Exclusions apply to all sections of the **policy**.

We will not pay any amount or be liable for any loss, damage, expense or benefit under this **policy** directly or indirectly based upon, arising from, attributable to, or as a consequence of:

1. physical damage to or the repair or replacement of **your** tangible property or equipment except to the extent covered under Optional Cover Section B4 - Tangible Property Cover if cover is elected.
2. any **loss, cyber event, system failure**, fact or circumstance known to **you** or discovered by **you** before the **policy period**.
3. any intentional, criminal, or fraudulent acts by **you** except to the extent covered under Extension A1 – Dishonesty or Fraudulent Act of Another Insured. For purposes of applying this exclusion, the acts, knowledge or conduct of any person(s) covered under this **policy** will not be imputed to any other person(s) covered under this **policy**.
4. **your** bankruptcy, liquidation or insolvency; or the bankruptcy, liquidation or insolvency of any **IT supplier** or external suppliers.
5. or resulting in, or causing an **employment wrongful act.**
6. any:
    a. ionising, radiation or contamination by radioactivity from any nuclear fuel, waste or other hazardous properties of any nuclear assembly or component,
    b. pollution, except to the extent covered under Section D – Public and Product Liability,
    c. electromagnetic field, electromagnetic radiation or electromagnetism.

7. a. **war**; and/or

   b. **cyber operation** that is carried out as part of a **war**, or the immediate preparation for a **war**; and/or

   c. **cyber operation** that causes a sovereign state to become an **impacted state**.

   Paragraph 7.c. will not apply to the direct or indirect effect of a **cyber operation** on a **computer system** used by **you** or **your** third party service providers that is not physically located in an **impacted state** but is affected by a **cyber operation**.

   Notwithstanding **our** burden of proof, which shall remain unchanged by this clause, in determining attribution of a **cyber operation** to a sovereign state, **you** and **we** will consider such objectively reasonable evidence that is available to **you** and **us**. This may include formal or official attribution by the government of the sovereign state in which the **computer system** affected by the **cyber operation** is physically located to another sovereign state or those acting at its direction or under its control.

8. any **act of terrorism**, except for **act of cyber terrorism** (but only in respect of Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others).

9. any damages characterised or described as aggravated, punitive or exemplary damages except to the extent covered under Section A – Professional Indemnity and Section C – Your Cyber Liability to Others.

10. any joint venture or consortium in which **you** have an interest, except for the legal liability arising solely out of:

    a. **your** conduct, act, error, omission or contribution to such joint venture or consortium, or

    b. **cyber event**, a breach of **computer system** security, **Payment Card Industry liability** caused by **you**.

11. any **claim** made by one **insured** against any other **insured** under this **policy**, or against **you**:

    a. by **your** partner,

    b. by **your** joint venture or consortium,

    c. by **your** parent company,

    d. by **your subsidiary**,

    e. by anyone or entity with effective control over **you**, or

    f. by any entity which **you** have effective control over or interest in.

    This exclusion will not apply to:

    a. Section D – Public and Product Liability of the **policy**, and

    b. liability arising from unintentional breach of confidentiality or breach of privacy of employees.

12. any actual or alleged infringement of any patent, except to the extent covered under Section A – Professional Indemnity up to the maximum of specified **limit** under infringement of patent rights noted on **your schedule**. **We** will not be liable for any patent claims, disputes, costs, expenses, arising from United States of America, their territories or possessions.

13. the redesign, rectification, or repair of any **product** defects.

14. the recall of **products** except to the extent covered under Extension D1 – Product Recall Expenses.

15. any capital gain or loss due to **your** inability to trade, invest, divest, buy or sell any financial security or financial asset of any kind.

16. an action brought against **your** directors or officers acting in that capacity except to the extent covered under Section C2 – Directors & Officers, if cover is elected.

Exclusions – Policy Section A Only

The following exclusions apply to Section A – Professional Indemnity only.

We will not pay any amount or be liable for any loss, damage, expense or benefit under this **policy** directly or indirectly based upon, arising from, attributable to, or as a consequence of:

17. violation of regulations relating to anti-trust, unfair competition, deceit, monopolisation, price fixing, predatory pricing, price discrimination, restraint of trade, or unfair business practices.

18. violation of Unsolicited Electronic Messages Act 2007 or similar legislation governing unsolicited communications.

19. enforcing or pursuing a breach of **your** intellectual property rights against a third party with which **you** have had an intellectual property related dispute in the five (5) years preceding the inception of the **policy period**.

20. the procurement, maintenance or collation of any intellectual property rights or monitoring for infringement of any intellectual property rights, which are not specifically occasioned by a covered claim under Extension A6 – Intellectual Property Pursuit Costs.

21. an opposition or observation made to any national or international intellectual property office to prevent the granting of or restrict the scope (pre-grant) of intellectual property rights.

22. enforcing or pursuing a breach of confidentiality or unlawful disclosure of trade secrets by a third party with which **you** have entered into an agreement.

23. any **professional services** by **you** or on **your** behalf as an accountant, lawyer, solicitor, barrister, architect, surveyor, health care provider, civil or structural engineer, financial or investment advisor, insurance advisor, and real estate agent.

Exclusions – Policy Section A and Section C Only

The following exclusions apply to Section A – Professional Indemnity and Section C – Your Cyber Liability to Others only.

We will not pay any amount or be liable for any loss, damage, expense or benefit under this **policy**:

24. for any actual or alleged **personal injury** or **property damage**. This exclusion shall not apply to mental illness as a result of a **cyber event** and for which **you** are legally liable for under Section C – Your Cyber Liability to Others.

Exclusions – Policy Section B and Section C Only

The following exclusions apply to Section B – Your Own Cyber Losses and Section C – Your Cyber Liability to Others only.

We will not pay any amount or be liable for any loss, damage, expense or benefit under this **policy** directly or indirectly based upon, arising from, attributable to, or as a consequence of:

25. physical cause or natural peril, such as fire, wind, water, flood, lightning, electromagnetism, explosion, collision, subsidence, earthquake, solar flares or storms, or any other type of radiation, or act of God howsoever caused.
26. a regional, national or global outage, failure or malfunction of a **utility provider**.
27. a liability that was assumed by **you** under any contract unless **you** have a liability independent of the contract.

Exclusions – Section C2 Only

The following exclusion applies to Optional Cover Section C2 – Directors & Officers cover only.

28. **We** will not pay any amount or be liable for any loss, damage, expense, or benefit under Section C2 – Directors & Officers:
    a. if **you** are listed on the New Zealand Stock Exchange, if **your** shares are traded on any other exchange, or if **you** are pursuing any actual or proposed initial or subsequent public offering,
    b. for any **claim** arising out of, or made in the United States of America, its territories or possessions, or by, or on behalf of, **you** or any director or officer.

Exclusions – Policy Section D Only

The following exclusions apply to Section D - Public and Product Liability only.

We will not pay any amount or be liable for any loss, damage, expense or benefit under this **policy** directly or indirectly based upon, arising from, attributable to, or as a consequence of:

29. asbestos, silica, or any dust or particles containing asbestos or silica.
30. **your** ownership, operation, or use of any aircrafts, hovercrafts, or drones that are weighing or carrying more than 15 kilograms, including any of **your products** that are incorporated, installed, or assembled as parts, or system that are connected with the operation, safety, flying capabilities, navigation, propulsion, fuel, or power system of such aviation crafts.
31. **your** ownership, operation, or use of any watercrafts or waterborne vessels that are more than 15 metres in length.
32. any liability arising from **personal injury** of an **insured** person where **you** would be entitled to indemnity under a workers' compensation insurance, regardless of whether such insurance has been carried out.
33. the operation or use of a vehicle owned by **you** or in **your** physical or legal control
    a. which is required by law to be registered, or
    b. in respect of which insurance is required by virtue of any legislation,

    but this exclusion does not apply to:
    a. **personal injury** or **property damage** caused by the use any vehicle as a tool, equipment, or plant for the conduct of **your business**.
    b. **personal injury** or **property damage** caused by the loading or unloading of goods from a vehicle or trailer during the conduct of **your business** when carried out beyond the limits of any carriageway or thoroughfare.
34. a **loss** where an individual is entitled to be covered or paid under the Accident Compensation Act 2001.

Section G – Claims Conditions

The following Claims Conditions apply to all sections of the **policy**.

You must comply with the following conditions if a **claim** is made against **you**, if **you** believe **you** have a claim under this **policy**, or if **you** discover a **cyber event** or **system failure**. If **you** do not comply with the following Claims Conditions, **we** may refuse to pay a **claim** in whole or in part.

1. In the event **you** become aware of a **claim** made against **you**, or an incident or **occurrence** which may give rise to a **claim**, then **you** must give **us** notice in writing at **claims@emergenceins.co.nz** as soon as practicable to do so and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**.
2. In the event **you** become aware of a **cyber event**, **you** must immediately ring the Emergence cyber event reporting line on **0800 129 237 (that is 0800 1 CYBER)** or notify Emergence in writing at **claims@emergenceins.co.nz** and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**.
3. **You** must notify **cyber theft**, **socially engineered theft**, **identity-based theft**, **push payment theft, telephone phreaking** or **cryptojacking** to, respectively, the National Cyber Security Centre, **your** financial institution, and **your** telephone service provider, within 24 hours of it first being discovered by **you**.

4. **We** will assess whether cover applies under **your policy**. **We** may at **our** discretion appoint an external claim investigator to assist **us** with a claim or a forensic investigator to assist **us** in determining if there is a **cyber event** or **system failure** and assess whether cover applies under **your policy**. If **we** do not appoint claim investigator or forensic investigator, **you** can with **our** prior **consent** and approval appoint a claim investigator or forensic investigator. The costs of the claim investigator and forensic investigator are included in the **limit** that applies under the **policy**.
5. **You** must do everything reasonably possible to preserve evidence to enable **us** to properly assess and investigate the claim.
6. If the claim is not covered under **your policy**, **we** will advise **you** to engage **your** own service resources.
7. **You** are required to fully cooperate with any reasonable requests made by **our** technical management, claims management and investigation teams and with any providers **we** appoint.
8. **You** must do everything reasonably possible to assist in the reduction or mitigation of the **impact on business costs, loss, cyber event response costs,** or **direct financial loss**.
9. **You** must, at **your** own cost, provide all necessary information to **us** to enable **us** to assess the claim and potential payment.
10. **We** may at **our** own discretion appoint an auditor to review and audit any **Payment Card Industry liability**.
11. If **you** do not accept **our** assessment of **impact on business costs** and **we** agree to **you** incurring **preparation costs, we** will pay up to a maximum amount of $10,000 for **preparation costs**.
12. **You** must obtain **our** prior **consent** before incurring or making payments.
13. **You** must obtain **our** prior written **consent** before incurring **defence costs** and obtaining **legal advice**.
14. **You** will pay the **excess** set out in **your schedule** before **we** pay or incur a payment.
15. If cost is incurred in response to any claim that is both covered and not covered under the **policy**, **we** and **you** will mutually agree on a fair and reasonable allocation of cost between what is covered and what is not covered under the **policy**. **We** will only pay the cost for any covered portion under the **policy**. In the event of a dispute as to a fair and reasonable allocation, such dispute may be referred by **you** or **us** to an appropriately qualified senior counsel (the costs to be paid by **us**). Their determination will be based upon written submissions only and will be final and binding. If an appropriately qualified senior counsel cannot be mutually agreed between **you** and **us**, the parties will request that the NZ Bar Association nominate a suitably qualified senior counsel and the parties agree to accept that nomination unconditionally.
16. If **you** suffer a **direct financial loss** as a result of **cyber theft**, **socially engineered theft, identity-based theft** or **push payment theft** and **you** are actively pursuing the recovery of the funds through **your** financial institution, **we** will pay the claim within thirty (30) calendar days of the claim being notified to **us**.
17. **You** must cooperate with and assist **us** in **our** attempts to recover **your direct financial loss**.
18. **You** must not admit any liability or agree to any judgement or settlement without **our** prior written **consent**.
19. **We** may refuse to pay any claim which is in any respect fraudulent or if any fraudulent means or devices are used by **you** or anyone acting on **your** behalf to obtain any benefit under this **policy**.
20. If **you** notify a claim, a **cyber event**, or a **system failure** to **us**, and either, or all, of i**mpact on business costs, loss, cyber event response costs**, or **direct financial loss** are incurred then **we** will apply the **aggregate** and **excess** set out in **your schedule** as if one such event happened.
21. All notified incidents and claims attributable to the same cause, event, **occurrence**, or a series of related, repeated, continuous event, act, error or omission, will be deemed as one claim. The "any one claim" **limit** or "any one occurrence" **limit** set out on **your schedule** will be the maximum **we** will pay for any one claim.
22. All notified incidents and claims which arise out of one **cyber event** or **system failure**, or a series of **cyber events** or **system failures** will be deemed to be one **cyber event** or **system failure**. The "any one claim" **limit** set out on **your schedule** will be the maximum **we** will pay for any one claim.
23. The notification to **us** of an incident or claim under one section of this **policy** will be deemed a notification to **us** under each section of the **policy**.

Section H – General Conditions

The following General Conditions apply to all sections of the **policy**.

1. **You** must comply with the conditionals of this **policy** at all times. If **you** or any other person or entity **we** cover under this **policy**, or anyone acting on **your** behalf breaches any of the terms and/or conditions of this **policy**, **we** may:
   a. refuse to pay a claim in whole or in part, and/or
   b. declare this **policy** or all insurance **you** have with **us** to be of no effect and to no longer exist.
2. True statements and answers must be given, whether by **you** or any other person, when:
   a. applying for this insurance, and/or
   b. notifying **us** regarding any change in circumstances, and/or
   c. making any claim under this **policy** and communicating with **us** or providing any further information regarding the claim.

3. 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**.
   d. **You** also have this duty every time **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.
4. **You** must notify **us** in writing as soon as practicable of any substantial change in **your business**.
5. **You** must notify **us** in writing as soon as practicable of any material alteration to the risk during the **policy period** including:
   a. if **you** go into voluntary bankruptcy, receivership, administration or liquidation;
   b. if **you** become aware of a pending appointment of a receiver or the commencement of bankruptcy or winding up proceedings to **your business**; or
   c. if **you** form or acquire an entity that does not meet the criteria for automatic inclusion under this **policy** as set forth in the definition of **subsiary**.
6. **You** must maintain IT security practices and procedures to a standard equal or better than **you** had in place at the time this **policy** commenced. A failure to adhere to such practices and procedures by an employee or an external supplier will not constitute a breach of this condition.
7. If during the **policy period** any other entity gains control of management or acquires more than 50 percent of the **policyholder** or any **subsidiary**, this **policy** will only respond to **loss** from a **claim** that happened prior to the date of such gaining of control or acquisition, unless **we** agree to extend coverage under the **policy** and **you** agree to the terms of any such extension of coverage.
8. This **policy** and any rights under it cannot be assigned without **our** written **consent**.
9. Where GST is recoverable by us under the Goods and Services Tax Act 1985:
   a. all **limits** exclude GST, and
   b. all sublimits exclude GST, and
   c. all **excesses** include GST, and
   d. GST will be added, where applicable, to claim payments.
10. The cancellation procedure is:
    a. By the **policyholder**
    The **policyholder** may cancel this **policy** at any time by notifying **us** in writing. **We** will refund any premium that is due to the **policyholder** based on the unused portion of the **policy period.** The **policyholder** must pay any outstanding premium due for the expired portion of the **policy period**.
    b. By **us**
    We may cancel this **policy** by giving the **policyholder**, or their broker, notice in writing or by electronic means, at the **policyholder's**, or their broker's last known address. The **policy** will be cancelled from 4pm on the 30th day after the date of the notice. **We** will refund the **policyholder** any premium that is due to them based on the unused portion of the **policy period**.
    c. Any premium owing to **us** under this **policy** must be paid to **us** within 60 days of the commencement of this **policy**. If the premium remains unpaid after the 60 day period. The **policy** will be cancelled from 4pm on the 30th day after the date of the notice.
11. If **we** make a payment under this **policy**, then **we** are entitled to assume **your** rights against any third party to the extent of **our** payment. **You** must, at **your** own cost, assist **us** and provide necessary information to **us** to enable **us** to bring the subrogation or recovery of a claim.
12. If an award or settlement is made in **your** favour, including an award relating to **defence costs**, in connection with a cover, **you** must provide prompt reimbursement (up to the amount of such award or settlement and no more) to **us** of any covered claim which **we** have paid or have an obligation to pay under this **policy**.
13. If any claim arises under this **policy** and there is any other insurance, which is more specific, that has been effected by **you**, or on **your** behalf, or of which **you** are a beneficiary, which covers the same loss in full or in part, then subject only to the terms and conditions of this **policy**, cover under this **policy** will apply in excess of such other insurance to the extent permitted by law. **You** are required to provide **us** details of the other insurance.
14. All premiums, **limits, loss,** costs and other amounts under this **policy** are expressed and payable in New Zealand dollars. Except as otherwise provided, if judgement is rendered, settlement is denominated or another element of loss under this **policy** is stated in other than New Zealand dollars, payment under this **policy** will be made in New Zealand dollars at the cash rate of exchange for the purchase of New Zealand dollars in accordance with the Reserve Bank of New Zealand on the date final judgement is reached, the amount of the settlement is agreed upon or the other element of loss becomes due.
15. Where **you**:
    a. prior to the **policy period** first became aware of facts or circumstances that might give rise to a **claim**; and
    b. did not notify **us** of such facts or circumstances prior to the **policy period**; and

c. **your** failure to notify **us** did not involve any deceptive or fraudulent intent; and

d. have been continuously insured under a **policy** issued by **us**, or by a similar policy issued by others, without interruption since the time **you** first became aware of such facts or circumstances;

then **we** will accept the notification within the **policy period** subject to:

a. the terms, conditions and **limits** of the **policy** in force when **you** first became aware of facts or circumstances that might give rise to the **claim** – if **you** have been continuously insured under a **policy** issued by **us**, or

b. the terms, conditions and **limits** of the first incepted **policy** with **us** – if **you** have been continuously insured under a similar policy issued by other insurers. This extension will not entitle **you** to a more extensive coverage than stipulated under **our policy**.

16. If this **policy** is terminated by either **us** or **you** for any reason other than non-payment of premium and no claim has been made and no other similar insurance has been arranged, then **you** will have the right to an extended reporting period for a period of thirty (30) calendar days for no additional premium. In the event of an extended reporting period, coverage otherwise afforded by this **policy** under Section A – Professional Indemnity and Section C – Your Cyber Liability to Others will be extended to apply to **claims** first made against **you** and notified to **us** during the extended reporting period arising out of a **cyber event**, **Payment Card Industry liability**, or any **loss** that happened prior to termination.

17. The insurers accepting this insurance agree that:

    a. if a dispute arises under this **policy**, this **policy** will be subject to New Zealand law and practice and **we** will submit to the exclusive jurisdiction of any competent court in New Zealand;

    b. any summons notice or process to be served upon **us** may be served upon:

    Lloyd's General Representative in New Zealand, C/O Hazelton Law

    PO Box 5639
    Wellington, New Zealand
    Telephone: +64 4 472 7582
    who has authority to accept service and to appear on **our** behalf;

    c. if a suit is instituted against any of the insurers, all the insurers participating in this **policy** will abide by the final decision of such Court or any competent Appellate Court.

18. The subscribing insurers' obligations under contracts of insurance to which they subscribe are several and not joint and are limited solely to the extent of their individual subscriptions. The subscribing insurers are not responsible for the subscription of any co-subscribing insurer who for any reason does not satisfy all or part of its obligations.

19. Sanctions Limitation Clause

    No (re)insurer will be deemed to provide cover and no (re)insurer will be liable to pay any claim or provide any benefit hereunder to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose that (re)insurer to any sanction, prohibition or restriction under United Nations' resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom, United States of America, New Zealand or any trade or economic sanctions, laws or regulations of any other jurisdiction.

20. **We** will have the duty to defend **you** against any **claim** **you** are legally liable for under this **policy** and the rights to take control of any investigation or settlement of any **claim** on **your** behalf. **We** will not settle any **claim** without **your** prior agreement, however, if **you** refuse a settlement which **we** recommend and the claimant will accept, then **you** must continue to defend the **claim** at **your** own cost. Provided that **you** are successful in defending the **claim**, **we** will reimburse **you** the cost related to **your** defence. However, **our** maximum liability will not be more than the amount which **we** would incur if **you** had agreed to the settlement.

21. **Defence costs** paid under:

    a. Section A – Professional Indemnity and Section C – Your Cyber Liability to Others can be either "inclusive" of **limit** or "in addition" to **limit** as stated in **your schedule**.

    b. Section D – Public and Product Liability will be "in addition" to **limit** except for **claims** occurring in the United States of America, its territories or possessions, where the **defence costs** will be paid inclusive of the **limit**.

    When **defence costs** are paid "in addition" to **limit**, the maximum **defence costs we** will pay will be the same as the **limit you** purchased under that section of the **policy**.

22. If during the term of the **policy you** become aware of any circumstance which may subsequently give rise to a **claim** against **you** then **you** shall during the **policy period** give written notice to **us** of the circumstance, then any such **claim** which may subsequently be made against **you** arising out of such circumstances shall be deemed to have been made during the **policy period**.

23. Any enquiry or complaint relating to this **policy** should be referred to Emergence NZ Limited in the first instance. If this does not resolve the matter or the **policyholder** is not satisfied with the way the enquiry or complaint has been dealt with, the **policyholder** should write to:

    Lloyd's General Representative in New Zealand
    C/O Hazelton Law
    PO Box 5639 Wellington, New Zealand
    Telephone: +64 4 472 7582

emergence

YOUR AWARD-WINNING UNDERWRITING AGENCY

0800 129 237

Level 11, Shortland Centre, 55 Shortland Street, Auckland 1010

emergenceinsurance.com