emergence

Cyb@r Event Protection

CEP-004.3 NZ
General Information
& Policy Wording

Contents

emergence

Cyber Event Protection CEP-004.3 NZ
General Information & Policy Wording

Published October 2023

General Information

About the Insurer

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

About Emergence NZ Limited

Emergence NZ Limited (Emergence) acts under a binding authority given to it by Certain Underwriters at Lloyd's (the underwriters) to administer and issue policies, alterations and renewals. In all aspects of arranging this **policy**, Emergence acts as an agent of the underwriters and not the **policyholder**.

Emergence 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

Emergence – the story

Emergence Insurance Pty Ltd launched in Sydney in April 2015. It has grown to be one of the largest providers of cyber insurance in Australia.

Emergence is a Lloyd's coverholder and a specialist cyber insurer. Cyber is all it does. It has been distributing cyber insurance through a white label agreement in New Zealand for 6 years. Now is the time to launch Emergence NZ Limited and have a presence in New Zealand.

How this policy works

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**.

It is important to understand the type of cover **you** have purchased and how the **limits** apply. Not every financial **loss** caused by a **cyber event** is covered under the **policy**. The type of losses covered are set out in Sections A, B and C. Section D sets out **our** Optional Covers that **we** may agree to.

Section A – Losses To Your Business

Section B – Loss To Others

Section C – Cyber Event Response Costs

Section D – Optional Covers

Optional Covers may be available. There is an additional premium payable by **you** to **us** for each Optional Cover. **Your schedule** will list the Optional Covers chosen by **you** that **we** have agreed to provide. The **limit**, or sublimit, and **excess** for each Optional 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**. The meaning of the words "**cyber event**" is also explained.

Section F – Exclusions sets out what the **policy** does not cover. These are the **policy's** exclusions.

How to Notify Us if a Cyber Event Happens or a Claim is Made Against You:

1. **You** must immediately ring the Emergence reporting line on 0800 129 237 (that's 0800 1 CYBER) or notify Emergence in writing at **claims@emergenceins.co.nz** and provide details and circumstances of the event, including any **claim** demand or notice received by **you** or proceedings against **you**.
2. **You** must report **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**.
3. **We** will assess whether cover applies under **your policy**.
4. **You** must do everything reasonably possible to preserve evidence to enable **us** to properly assess and investigate the claim.
5. 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.*

Note: *This* ***policy*** *does not cover equipment breakdown, property damage or the cost of replacement of tangible property or equipment.* ***Claims*** *arising from the rendering or failure to render professional services, or for liability while acting as an* ***IT contractor*** *or in the capacity as a fiduciary or director or officer, are not covered. This* ***policy*** *is not a substitute for fidelity or comprehensive crime insurance.* ***You*** *should speak to your insurance broker about what this* ***policy*** *covers and what other insurance covers* ***you*** *need.*

Section G – Claims Conditions

Explains what **you** must do if there is a **cyber event**.

Section H – General 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 or 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

This **policy** wording and **your schedule**, which includes any endorsements, determine the cover **we** provide **you** under this **policy**. It is important that **you** read and understand the **policy** in its entirety.

We will pay up to the **limit** or sublimit stated in the **schedule** for each of Sections A, B and C and for any Optional Cover. The **aggregate** is the most **we** will pay for all Sections, including any Optional Covers. The **limit** stated in **your schedule** is exclusive of GST.

Section A – Losses To Your Business

If a **cyber event** happens in **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**.

If a **preventative shutdown** happens during the **policy period**, **we** will pay **you** a **preventative shutdown allowance**.

Section B – Loss 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 **multimedia injury** or because of a **cyber event** in **your business**.

Section C – Cyber Event Response Costs

If 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 pay **your cyber event response costs**.

Section D – Optional Covers

Optional Cover is only provided if stated in **your schedule**. Each Optional Cover is subject to all other terms of the **policy** unless otherwise stated in the Optional Cover.

The **limit** or sublimit and **excess** for each Optional Cover, if applicable, will be stated in **your schedule** exclusive of GST and is the maximum **we** will pay in any one **policy period** for all claims under that Optional Cover. Optional Cover **limits** form part of and are included within the **aggregate**.

Optional Cover – Contingent Business Interruption Cover

We will pay **you impact on business costs** caused by:

a. **supplier outage**, or

b. **system failure**.

For the purpose of this Optional Cover – Contingent Business Interruption Cover only the words listed below have been given a specific meaning and the specific meanings apply:

cyber event is extended to include a **cyber event** at **your** direct external supplier's business.

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 **supplier outage** or a **system failure**, less any consequent savings, and less any **delayed revenue**, plus

b. the net increased costs incurred during the **indemnity period** to avoid a reduction in **revenue** directly as a result of the interruption to **your business** 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** request.

We will not pay any **impact on business costs** incurred under this Optional Cover – Contingent Business Interruption Cover during the waiting period of three days (72 hours) after the first interruption to **your business**.

indemnity period is amended and means the continuous period starting from the first interruption to **your business** until:

a. supply from **your** direct external supplier resumes, or until **you** have a substitute supply (in the case of **supplier outage**), or

b. the outage is sufficiently restored to support **your** usual **business** operations (in the case of **system failure**)

plus reasonable additional time to allow **your business** to normalise. The **indemnity period** shall not exceed a total length of 35 days.

supplier outage means an interruption to **your business** directly arising from an outage at **your** direct external suppliers' business, where, in **our** opinion, the outage has been caused by a **cyber event** at **your** direct external supplier's business.

system failure means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **your IT** or **IT** under the direct control of **your IT contractor**, 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 **your IT**;

d. falling within parameters of a service level agreement; or

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

The maximum **limit we** will pay in any one **policy period** under this Optional Cover – Contingent Business Interruption Cover is $250,000 unless another amount is stated in **your schedule**.

Optional Cover – Criminal Financial Loss Cover

We will pay a **direct financial loss** to **you** or a **direct financial loss** to others 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**

that is first discovered by **you** and notified to **us** in the **policy period**.

Section F – Exclusion 17 of the **policy** is varied to the extent of this Optional Cover – Criminal Financial Loss Cover.

For the purposes of this Optional Cover – Criminal Financial Loss Cover only, **we** will pay **pursuit costs** of up to a maximum of $50,000 paid with **our** agreement and 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 perpetrator of a **cyber theft**, **socially engineered theft**, **identity-based theft**, **push payment theft telephone phreaking** or **cryptojacking**.

For the purposes of this Optional Cover – Criminal Financial Loss Cover only, the words listed below have been given a specific meaning and these specific meanings apply:

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 currencies, gift cards, vouchers, coupons or reward points.

investigation costs means costs **you** incur with **our** prior consent to investigate and substantiate the circumstances and amount of a **socially engineered theft** covered under this Optional Cover – Criminal Financial Loss Cover. **Investigation costs** are included in the **limit** for Optional Cover – Criminal Financial Loss Cover.

You must report the **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**.

The maximum **limit we** will pay in any one **policy period** for all **direct financial loss** under this Optional Cover – Criminal Financial Loss Cover is stated in **your schedule**. This includes all claims for **socially engineered theft.** The sublimit for any **claim** or series of related claims for **socially engineered theft** is stated in **your schedule** and is the maximum **we** will pay for all **socially engineered theft** in any one **policy period**.

The **excess** for this optional cover is set out in **your schedule.**

Optional Cover – Tangible Property Cover

We will pay the cost of the replacement or repair of **your** IT hardware that is physically damaged or no longer suitable for use solely and directly because of a **cyber event** covered under this **policy** or the incurring of related **cyber event response costs**.

Section F – Exclusion 1 of the **policy** is varied to the extent of this Optional Cover – Tangible Property Cover.

Optional Cover – Joint Venture and Consortium Cover

The cover provided under Section B – Loss To Others section of this **policy** is extended to **your** participation in a joint venture or consortium **you** have declared to **us**.

This Optional Cover – Joint Venture and Consortium Cover applies only if **you** have declared to **us** the estimated total **revenue** to be received from the joint venture or consortium for the coming 12 month period and the joint venture or consortium is named in **your schedule**.

This Optional Cover covers **you** only. No other participant in such joint venture or consortium, and no other third party, has any rights under this **policy**, nor shall **we** be liable to pay a contribution to any insurer of any other participant in such joint venture or consortium.

Section F – Exclusion 19 of the **policy** is varied to the extent of this Optional Cover – Joint Venture and Consortium Cover.

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.

act(s) of terrorism includes any act which may or may not involve the use of, or threat of, force or violence where the purpose of the act is to further a political, religious, ideological aim or to intimidate or influence a government (whether lawfully constituted or not) or any section of the public.

aggregate means the most **we** will pay, including **defence costs**, in any one **policy period** for all **cyber event**s, **losses**, **claims**, **preventative shutdowns**, **investigation costs** or **direct financial loss** for all insureds, under Sections A – Losses To Your Business, Section B – Loss To Others and Section C – Cyber Event Response Costs and any Optional Covers taken out by **you**. The **aggregate** is stated in **your schedule**. All **limits** and sub-limits are included in and form part of the **aggregate**.

business means the **policyholder's business** set out in **your schedule**. The **policyholder** must be domiciled in or operate from New Zealand.

business activity means the activity carried on by **your business** set out in **your schedule**.

claim means any written demand, notice of pending action or civil, criminal, administrative, regulatory or arbitral proceedings against **you** seeking compensation or other legal remedy caused by or in connection with a **cyber event** or **multimedia injury**.

computer system, for purposes of exclusion 10, 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.

cryptojacking means the unauthorised use of **your IT** to mine digital currency that causes **you direct financial loss**.

cyber event must happen in **your business** and means the following:

- **crimeware** which is any malware of any type intentionally designed which causes harm to **your IT** but does not include **cyber espionage** or **point of sale intrusion**.
- **cyber espionage** which is unauthorised access to an item of **your IT** linked to a state affiliated or criminal source exhibiting the motive of espionage.
- **cyber extortion** which is a crime involving an attack or threat of attack against **your IT**, or data in **your IT**, coupled with a demand for money or other valuable consideration (including digital currency) to avert or stop the attack.
- **denial of service** which is uniquely intended to compromise the availability of **your IT**. This includes a distributed **denial of service**.
- **hacking** which is malicious or unauthorised access to **your IT**.
- **insider and privilege misuse** which is unapproved or malicious use of **your IT** by **your** employees, outsiders in collusion with **your** employees, or business partners who are granted privilege access to **your IT** but does not include theft, **socially engineered theft**, **identity-based theft, push payment theft** or **cyber theft**.
- **miscellaneous errors** where unintentional actions directly compromise a security attribute of an item of **your IT** but does not include theft, **socially engineered theft** or **cyber theft**.
- **privacy error** where acts or omissions by **your** employees lead to unauthorised access to, unauthorised disclosure of or loss of data (including non-electronic data) which necessitates incurring **notification costs** or **identity theft response costs**.
- **payment card skimming** involving a skimming device being physically implanted through tampering into an item of **your IT** that reads data from a payment card.
- **physical theft and loss** where an item of **your IT** is missing or falls into the hands of a third party or the public whether through misplacement or malice.
- **point of sale intrusion** being a remote attack against **your IT** where retail transactions are conducted, specifically where purchases are made by a payment card.
- **web app attacks** where a web application was the target of attack against **your IT**, including exploits of code level vulnerabilities in the application.

cyber event response costs means the reasonable costs and expenses being:

- **credit and identity monitoring costs** incurred in engaging monitoring services by a third party for persons affected by a **cyber event** for a period of up to 12 months.
- **cyber extortion** costs paid with **our** agreement and consent to respond to a **cyber event** where a third party is seeking to obtain pecuniary gain from **you** through **cyber extortion**.
- **data restoration costs** incurred in restoring or replacing **your** data, data **you** hold or process on behalf of others, or programs in **your IT** that have been lost, damaged or destroyed and the cost to mitigate or prevent further damage, and includes the cost of **you** purchasing replacement licences, if necessary, but does not include any costs relating to redesign, replication or reconstitution of proprietary information, facts, concepts or designs.
- **data securing costs** incurred in securing **your IT** to avoid ongoing **impact on business costs**, **loss** and **cyber event response costs**.
- **external management 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 **your IT** or to prevent reputational harm to **you**.
- **identity theft response costs** incurred in supporting an individual with reporting of the **identity theft** and re-establishing identity and essential records.
- **legal advice costs** reasonably and necessarily incurred with our written consent to advise **you** in the response to a **cyber event. Legal advice costs** do not include **defence costs.**
- **notification 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.
- **public relations costs** incurred in responding to a **cyber event** or to prevent reputational harm to **you** including external public relations, media, social media and communications management.
- **pursuit costs** of up to a maximum of $50,000 paid with **our** agreement and 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 perpetrator of a **cyber event** covered under this **policy**.
- **virus extraction costs** incurred to remove a virus from **your IT**.

cyber operation, for the purposes of exclusion 10, means the use of a **computer system** by, at the direction of, or under the control of a **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**.

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

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**.

delayed revenue means **revenue** earned in the period of 90 days after the end of the **indemnity period** which would have been earned during the **indemnity period** if the **cyber event** did not happen.

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**.

essential service, for the purposes of exclusion 10, means a service that is essential for the maintenance of vital functions of a **state** including, but not limited to, financial institutions and associated financial market infrastructure, health services or utility services.

excess means the amount of money that **you** are responsible for before **we** make a payment under the **policy**. The **excess**, including the **excess** for any Optional Cover, is set out in **your schedule**. If there is more than one **excess** stated in **your schedule** then **you** will pay the higher **excess** if the incident or claim relates to that higher **excess.**

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**.

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 IT**. **Identity theft** does not include **identity-based theft**.

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**, less any consequent savings, and less any **delayed revenue**, plus

b. the net increased costs incurred during the **indemnity period** to avoid a reduction in **revenue** directly as a result of a **cyber event** 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** request. **We** will not pay **impact on business costs** incurred during the waiting period of the first 12 hours after **you** discover a **cyber event** unless a different waiting period has been specified on **your schedule** or unless the first discovery of the **cyber event** occurred during a **preventative shutdown**.

impacted state, for the purposes of exclusion 10, means any **state** where a **cyber operation** has had a major detrimental impact on:

a. the functioning of that **state** due to the disruption to the availability, integrity or delivery of an **essential service** in that **state;** and/or

b. the security or defence of that **state**.

indemnity period means the period starting from discovery of the **cyber event** until **your IT** 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**.

IT contractor is a person contracted to provide, maintain, service or manage information technology services or infrastructure**.**

IT means all of the hardware, servers, systems, firmware, software, networks, platforms, facilities, and similar or related items, owned by or leased to, rented to or licenced to **you**, regardless of where it is hosted and whether it is operated by **you**, **your IT contractor** or in the cloud, insofar as they are required to develop, test, deliver, monitor, control or support IT services **you** use in **your business**. The term **IT** includes all of the information technology but not the associated people, processes and documentation.

limit means the amount set out in the **schedule** for each of Section A – Losses To Your Business, Section B – Loss To Others and Section C – Cyber Event Response Costs of **your policy** and applies to any one **cyber event**, irrespective of the number of **claim(s)**. The **limit** or sublimit for any Optional Cover is also set out in **your schedule**.

loss means any sums payable pursuant to judgements (including orders for costs), settlements, awards and determinations including damages, regulatory and civil fines and penalties in respect of a **claim**, and any costs as consequence of a mandatory notice from a regulatory authority as a consequence of the failure to secure information held by **you**. **Loss** includes **defence costs**.

multimedia injury means **loss** to others because of unintentional:

a. libel, slander, defamation;

b. infringement of trademark, service mark, slogan, copyright, domain name or metatags;

c. improper deep linking, framing, or web harvesting;

d. inadvertent disclosure of personal information;

solely occasioned through **your** website content, social media presence (including comments made by third parties for which **you** may be held legally responsible) or other online mediums. **Multimedia injury** does not include any actual or alleged infringement of any patent.

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 non-compliance after the initial monetary fine or assessment.

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

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

policyholder means the entity first named in **your schedule** under **Policyholder** / **Business** and is authorised to enter into and deal with this **policy** on behalf of all other entities covered under the **policy**.

preparation costs means the costs **we** will pay to assist **you** to verify **impact on business costs** incurred by **you**.

preventative shutdown means the reasonable, necessary and intentional shut down of **your IT** in response to a **cyber event** in **your business**, or a credible threat to **your IT** following:

a. a **cyber event** at **your** direct customer, supplier or business partner,

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

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 IT**.

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 to avoid a reduction in **revenue** directly as a result of a **preventative shutdown** 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.

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

Preventative shutdown allowance does not include **cyber event 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** request. **We** will not pay **preventative shutdown allowance** during the waiting period of the first 12 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 IT**; or

b. the safe resumption of operations of **your IT**.

The **preventative shutdown allowance** is set out in **your schedule** and is the maximum **we** will pay for all **preventative shutdowns** in any one **policy period**. It is included in and forms part of the **limit** for Section A – Losses To Your Business.

push payment theft means the fraudulent issuance of an invoice from **your IT** 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 to **your IT** and without **your** knowledge. **Push payment theft** does not include **cyber theft**, **socially engineered theft** or **identity-based theft**.

records of your business means 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.

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

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

socially engineered theft means an electronic transfer 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 IT**, having believed such facts to be genuine and true. **Socially engineered theft** does not include **cyber theft, push payment theft** or **identity-based theft**.

state, for purposes of exclusion 10, means sovereign state.

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** also includes entities **you** form or acquire during the **policy period** that meet the following criteria, but only for **cyber event**s 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 **cyber event**s, **losses** or claims prior to **you** acquiring it;

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

telephone phreaking means a **hacking** of **your business** telephone systems that causes you **direct financial loss**.

utility provider includes providers of gas, electricity, water, sewage, telecommunications, satellite, cable, internet access, internet backbone, DNS servers or other core infrastructure of the internet.

war, for the purposes of exclusion 10, means armed conflict involving physical force:

a. by a **state** against another **state**, or

b. as part of a civil war, rebellion, revolution, insurrection, military or usurpation of power,

whether war be declared or not.

we/**our**/**us** means certain underwriters at Lloyd's (the underwriters) as insurers of the **policy** and Emergence acting on behalf of underwriters as issuer of this **policy**.

Note: **You** can obtain further details of the underwriters from Emergence upon request.

you/**your** means the **policyholder** referred to in **your schedule**. It includes the **policyholder's subsidiaries**, any affiliates stated in **your schedule**, and 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. 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.

Section F – Exclusions

Exclusions - all policy sections

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

We will not pay any **impact on business costs**, **loss**, **cyber event response costs**, **direct financial loss** or **preventative shutdown allowance**, or be liable for any **loss**, damage, expense or benefit:

1. arising from or for physical damage to or the repair or replacement of tangible property or equipment.

2. arising from or as a consequence of death or bodily injury, however, this exclusion shall not apply to mental illness as a result of a **cyber event** and for which **you** are legally liable.

3. arising from any **cyber event**, **multimedia injury**, **loss**, fact or circumstance known to **you** or discovered by **you** before the **policy period**.

4. arising from or based upon any intentional, criminal or fraudulent acts by **you**. For purposes of applying this exclusion the acts, knowledge or conduct of any person covered under this **policy** will not be imputed to any other person covered under this **policy**.

5. arising from or as a consequence of **your** bankruptcy, liquidation or insolvency or the bankruptcy, liquidation or insolvency of any of **your IT contractor**s or external suppliers.

6. arising from, or resulting in, or causing an **employment wrongful act**.

7. arising from, attributable to, or as a consequence of ionising, radiation or contamination by radioactivity from any nuclear fuel, waste or other hazardous properties of any nuclear assembly or component.

8. arising from, attributable to, or as a consequence of pollution.

9. directly or indirectly involving the infringement of any copyright, service mark, trademark or other intellectual property, however this exclusion shall not apply to **multimedia injury** expressly covered under Section B.

10. directly or indirectly occasioned by, happening through, arising or in consequence of:

a. **war** and/or

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

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

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

Attribution of a **cyber operation** to a **state**

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

11. caused by or arising out of any **act of terrorism**, however, this exclusion does not apply to:

    a. the following **cyber events**:

       crimeware, **cyber espionage**, **cyber extortion**, **denial of service**, **hacking**, **payment card skimming**, **point of sale intrusion** or **web app attacks**; and

    b. Optional Cover – Criminal Financial Loss Cover.

    This exclusion does however apply to any such activities that are excluded under exclusion 10 (**war** or a **cyber operation**).

12. arising from, attributable to, or in consequence of any electromagnetic field, electromagnetic radiation or electromagnetism.

13. that was assumed by **you** under any contract unless **you** have a liability independent of the contract. This exclusion does not apply to a **Payment Card Industry Liability**.

14. that is related to damages characterised or described as aggravated, punitive or exemplary damages.

15. caused by defective equipment, ordinary wear or deterioration, faulty design or construction or insufficient capacity of **your IT**. This exclusion does not apply to a **system failure** caused by defective equipment.

16. arising out of or caused by outage of a **utility provider**.

17. arising from, attributable to, or as a consequence of **cyber theft**, **socially engineered theft**, **identity-based theft**, **push payment theft**, **telephone phreaking** or **cryptojacking**. This exclusion does not apply to **cyber event response costs** incurred solely and directly due to **cyber theft**, **identity-based theft**, **push payment theft**, **telephone phreaking** or **cryptojacking**.

18. to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose **us** or any (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 or United States of America.

19. arising from, attributable to, or as a consequence of any joint venture or consortium in which **you** have an interest.

20. in connection with any **claim** made by one insured against any other insured under this **policy**, or against **you** by **your** parent company or by anyone with effective control over **you**.

21. arising from, attributable to, based upon or in connection with any **claim**, **loss**, judgement or award made in the United States of America or which applied the laws of the United States of America.

22. directly or indirectly involving any actual or alleged infringement of any patent.

23. arising out of the recall, redesign or rectification of any products, hardware, software, software as a service, platform as a service, infrastructure as a service, or related services or IT **you** sell, lease, license or otherwise provide to others for a fee.

24. related to any warranty for any products, hardware, software, software as a service, platform as a service, infrastructure as a service, or related services or IT **you** sell, lease, license or otherwise provide to others for a fee.

25. arising from, attributable to, or as a consequence of 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.

26. arising out of physical cause or natural peril, such as fire, wind, water, flood, lightning, explosion, collision, subsidence, earthquake, solar flares or storms, or any other type of radiation, or act of God howsoever caused.

Exclusions - Section B of the Policy only

The following exclusions apply to Section B only.

We will not pay a **loss** that **you** are legally liable for arising out of a **claim** under Section B of the **policy:**

27. for an action:

    a. brought against **your** directors of officers acting in that capacity, or

    b. brought against **you** for an error or omission while acting in a professional or fiduciary capacity, or

    c. brought against **you** operating as an **IT contractor**.

28. in connection with any products, hardware, software, software as a service, platform as a service, infrastructure as a service, or related services or IT **you** sell, lease, license or otherwise provide to others for a fee.

Section G – Claims Conditions

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

1. **You** must immediately ring the reporting line on 0800 129 237 (that's 0800 1 CYBER) or notify Emergence in writing at claims@emergenceins.co.nz and provide details and circumstances of the event, including any demands or notices received by **you** or proceedings against **you**.
2. **You** must report **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**.
3. **We** will assess whether cover applies under **your policy**. **We** may at **our** discretion appoint a forensic investigator to assist **us** in determining if there is **cyber event** and assess whether cover applies under **your policy**. If **we** do not appoint a forensic investigator **you** can with **our** prior consent and approval appoint a forensic investigator. The costs of the forensic investigator are included in the **limit** that applies to the **cyber event**.
4. **You** must do everything reasonably possible to preserve evidence to enable **us** to properly assess and investigate the **claim**.
5. If the **claim** is not covered under **your policy**, **we** will advise **you** to engage **your** own service resources.
6. **You** are required to fully cooperate with **our** technical management, claims management and investigation teams and with any providers **we** appoint.
7. **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**.
8. **You** must, at **your** own cost, provide all necessary information to **us** to enable **us** to assess the **claim** and potential payment.
9. **We** may at **our** own discretion appoint an auditor to review and audit any **Payment Card Industry Liability**.
10. 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**.
11. **We** will not reimburse **you** for any costs incurred by or payments made by **you** unless approved by **us**.
12. **Defence costs** and **legal advice costs** must be approved by **us** in writing before they can be incurred by **you**. **We** will not unreasonably withhold **our** consent to **you** incurring reasonable and necessary **defence costs** or **legal costs**.
13. **You** will pay the **excess** set out in **your schedule** before **we** pay or incur a payment.
14. If cost is incurred in response to a **cyber event preventative shutdown, system failure, socially engineered theft** or **claim** and some of that cost is not **impact on business costs**, **preventative shutdown allowance, loss, cyber event response costs** or **direct financial loss** it is **your** responsibility to pay some or all of the cost. **We** will determine a fair and reasonable allocation of cost between what is covered and what is not covered under the **policy**.
15. If **you** suffer a **direct financial loss** as a result of **cyber theft**, **socially engineered theft**, **identity-based theft** or **push payment theft**, **we** can at **our** discretion and if the funds remain unrecoverable pay the **claim** within 30 days of the **claim** being notified to **us**.

    If **we** do elect to pay the **claim**, **you** must cooperate with and assist **us** in **our** attempts to recover **your direct financial loss**.

    If the funds are recovered and paid into **your** own account, **you** must immediately advise **us** and repay to **us** the funds recovered.

Section H – General Conditions

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

1. **You** must comply with the conditions 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 the insured has 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.

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

4. **You** must notify **us** in writing as soon as practicable of any change in **your business activity**.

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. **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 **subsidiary**.

   If **you** do notify **us** of a change, **we** may alter the premium, the terms of **your** insurance or cancel the insurance with effect from the date on which the change first occurred.

6. **You** must maintain IT security practices and procedures to a standard equal to or better than as existed at the time this **policy** commenced. A failure to adhere to such practices and procedures by an employee or **your IT contractor** shall 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** shall be restricted in respect of the **policyholder** or that **subsidiary** so as to apply only to **cyber events**, **multimedia injury** or **socially engineered theft** 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 sub-limits 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. **We** will indemnify **you** for claims under Section B – Loss To Others, where the **claim** is brought under the jurisdiction of any country where **you** are located, excluding the United States of America, its territories or possessions, or any judgement or award pursuant to United States law by the courts of any other country.

12. 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 claim.

13. If any claim arises under this **policy** and there is any other insurance that has been effected by **you**, or on behalf of **you**, or of which **you** are a beneficiary, which covers the same loss in full or in part, then **you** must promptly notify **us** of full details of such other insurance, including the identity of the insurer(s) and the policy number(s), and such further information as **we** may reasonably require. **We** reserve the right to seek a contribution from the other insurer(s).

14. **You** may not disclose the existence and terms of this **policy**. However, **you** may disclose the existence of this **policy** to the extent that **you** are required to do so by law or **you** need to prove **you** have the cover as part of a work tender or contract.

15. All premiums, **limits**, **loss** 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** shall 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.

16. If **you** report a **cyber event, preventative shutdown, system failure, socially engineered theft** or **claim** to **us** and either, or all, of **impact on business costs**, a **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.

17. All reported incidents and claims which arise out of one **cyber event** or a series of **cyber events** involving **your IT** or **business** will be deemed to be one **cyber event** and only one **aggregate** will apply.

18. 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** or any Optional Cover.

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

20. 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** shall have the right to an extended reporting period for a period of thirty days (30) for no additional premium. In the event of an extended reporting period, coverage otherwise afforded by this **policy** will be extended to apply to **claims** first made against **you** and notified to **us** during the extended reporting period arising out of **cyber events** or **multimedia injury** that happened prior to termination.

21. The underwriters accepting this insurance agree that:

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

    b. any summons notice or process to be served upon the underwriters may be served upon the Lloyd's Underwriters' General Representative in New Zealand,

    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 the underwriters' behalf;

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

    In the event of a claim arising under this **policy** NOTICE should be given to Emergence NZ Limited as soon as possible.

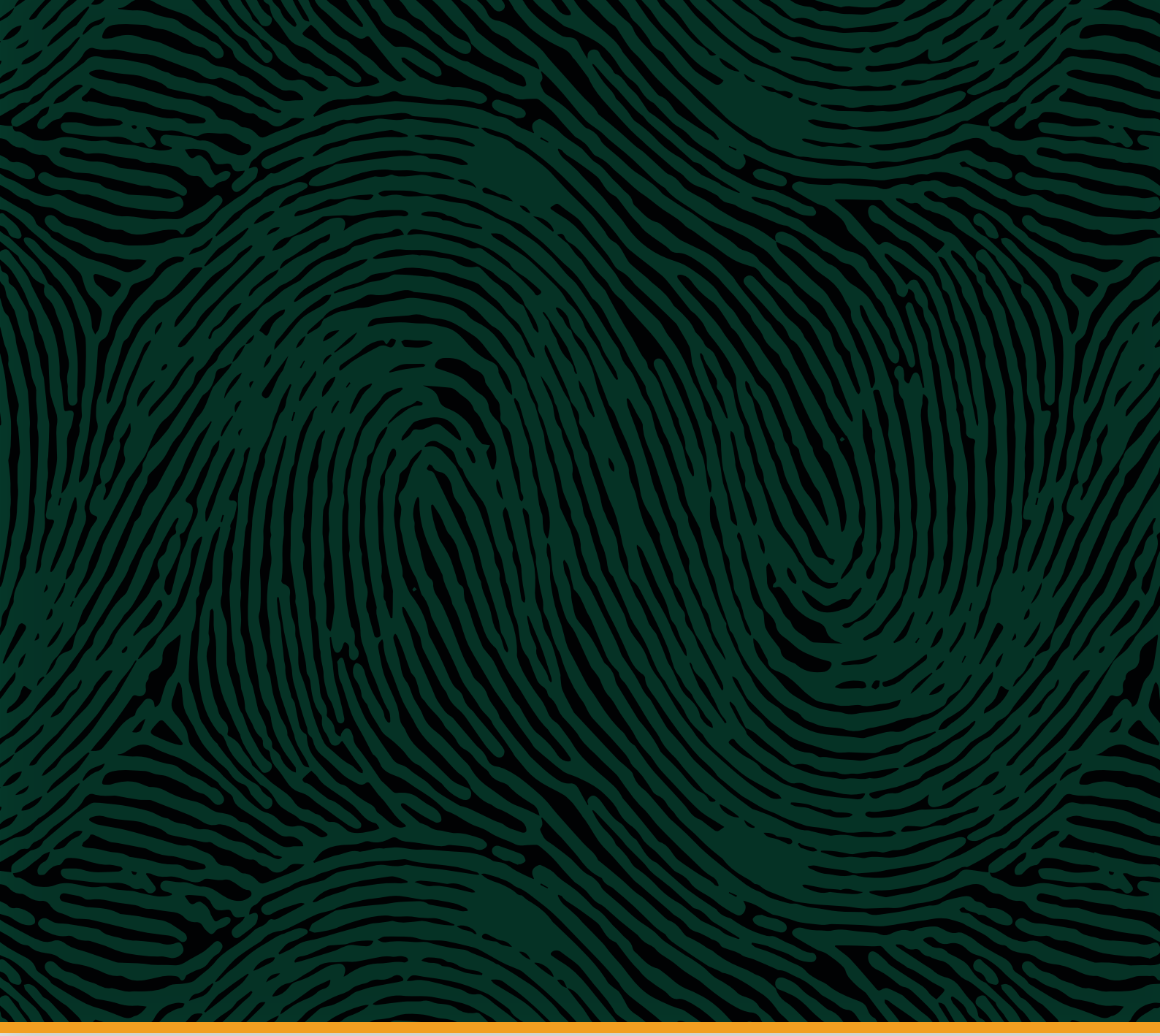
22. The subscribing insurers' obligations under contracts of insurance to which they subscribe are several and not joint and are limited solely to the extent of their individual subscriptions. The subscribing insurers are not responsible for the subscription of any co-subscribing insurer who for any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

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 NZ Limited October 2023



emergence

Level 11, Shortland Centre
55 Shortland Street
Auckland 1010

0800 129 237
emergenceins.co.nz