

emergence



Cyb@r Event Protection

—
Important Information
& Policy Wording



Contents

Important Information	3
About the Insurer	3
About Emergence Insurance Pty Ltd	3
Our Agreement	3
How this Policy Works	3
How to Notify Us if a Cyber Event Happens or a Claim is Made Against You	3
Claims Made Notice	4
Your Duty of Disclosure	4
Receiving Your Policy Documents	4
Words with Special Meaning	4
Headings	5
The Cost of Your Policy	5
Renewal Procedure	5
Your 'Cooling Off' Rights	5
Complaints	5
General Insurance Code of Practice	6
Privacy Statement	6
Policy Wording	7
Section A – Losses to Your Business	7
Section B – Loss to Others	7
Section C – Cyber Event Response Costs	7
Section D – Optional Covers	7
Section E – What Certain Words Mean	9
Section F – Exclusions	13
Section G – Claims Conditions	15
Section H – General Conditions	16

emergence

Cyber Event Protection
Important Information & Policy Wording

Published March 2021
© Emergence Insurance Pty Ltd

Important Information

This important information explains the cover provided by the **policy** wording and provides **you** with notices, but is not part of the **policy** wording. Please read both this important information and the **policy** wording.

Words or expressions in bold in this important information share the same meaning as they do in the **policy**.

About the Insurer

This insurance is underwritten by certain underwriters at Lloyd's. Lloyd's underwriters are authorised by the Australian Prudential Regulation Authority ('APRA') under the provisions of the Insurance Act 1973 (Cth).

If **you** require further information about this insurance or wish to confirm a transaction, please contact Emergence.

About Emergence Insurance Pty Ltd

Emergence Insurance Pty Ltd (ABN 46 133 037 153, AFSL 329634) [Emergence] acts under a binding authority given to it by **us** to administer and issue policies, alterations and renewals. In all aspects of arranging this **policy**, Emergence acts as an agent for **us** and not for **you**. Contact details are:

Email: info@emergenceinsurance.com.au
Telephone: +61 2 8280 3000
Postal address: PO Box A2016, Sydney South NSW 1235

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 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 "**cyber event**" is also explained.

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

1. **You** must immediately ring the Emergence **cyber event** reporting line on 1300 799 562 or notify Emergence in writing at claims@emergenceinsurance.com.au and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**.
2. **You** must report **cyber theft**, **socially engineered theft**, **identity-based theft**, **telephone phreaking** or **cryptojacking** to, respectively, the Australian 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.*

Section F – Exclusions

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

*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**.

Claims Made Notice

Section B – Loss To Others of this **policy** is issued on a 'claims made and notified' basis. This means that Section B – Loss To Others responds to:

- a. **claims** first made against **you** during the **policy period** and notified to **us** during the **policy period**, provided **you** were not aware at any time prior to the commencement of the **policy** of circumstances which would have put a reasonable person in **your** position on notice that a **claim** may be made against **you**; and
- b. written notification of facts pursuant to Section 40(3) of the *Insurance Contracts Act 1984* [Cth]. Effectively, the facts that **you** may decide to notify are those which might give rise to a **claim** against **you** even if a claim has not yet been made against **you**. Such notification must be given as soon as reasonably practicable after **you** become aware of the facts and prior to the expiry of the **policy period**. If **you** give written notification of facts, the **policy** will respond even though a claim arising from those facts is not made against **you** until after the **policy** has expired. When the **policy period** expires, no new notification of facts can be made to **us** on the expired **policy** for a **cyber event** or **multimedia injury** first discovered or identified by **you** during the **policy period**.

Your Duty of Disclosure

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

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

You have the same duty before **you** renew, replace, extend, vary, continue under a similar insurance or reinstate an insurance contract.

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

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

If you do not tell us something

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

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

Receiving Your Policy Documents

It is a condition of this **policy** that **you** shall receive **your policy** documents electronically only. If **you** are unable or unwilling to receive **your policy** documents electronically, **we** shall not enter into a contract of insurance with **you**.

Emergence will send **your policy** documents to the email address nominated by **you** or **your** agent. Each electronic communication will be deemed to be received by **you** 24 hours after it leaves Emergence's information system.

You are responsible for ensuring that the email address that Emergence has for **you** is up to date. Please contact Emergence to change **your** email address.

Words with Special Meaning

Some words and expressions used in the **policy** have special meanings. These words are always in bold. The meaning of words and expressions in bold are explained under the heading "What Certain Words Mean".

Headings

The headings of clauses the **policy** are for reference purposes only. They do not form part of the **policy**.

The Cost of Your Policy

The amount that **we** charge **you** for this **policy** when **you** first acquire it and when **you** renew **your policy** is called the **premium**. The **premium** is the total that **we** calculate when considering all of the factors which make up the risk. Depending on the frequency of claims the **premium** on renewal of the **policy** may be different to the premium for this **policy**.

The **premium** is subject to government taxes, levies and duties such as GST and Stamp Duty. Emergence may also charge a policy fee in addition to the **premium**.

The total cost of **your policy** is shown on the **schedule** and is made up of **your premium** plus government taxes, levies and duties (where applicable) and a **policy** fee (if applicable).

Renewal Procedure

Before this **policy** expires, **we** will advise **you** whether **we** intend to offer **you** a renewal and if so, on what terms. It is important to check the terms of any renewal before renewing it to ensure that the details are correct.

Your 'Cooling Off' Rights

You can return **your policy** to **us** within 14 days of its commencement, which is stated on **your schedule**. If **we** receive **your** written request to cancel this **policy** within the 14 day period, **we** will cancel the **policy** effective from the **policy period** commencement date and give **you** a full refund. **You** cannot use this right where, before the 14 day period ends, **you** have exercised any of **your** rights or powers under the **policy** (e.g. **you** have made a claim).

After the cooling off period ends **you** still have cancellation rights under the **policy** (see **our** General Conditions).

Complaints

Step 1:

Any enquiry or complaint relating to this insurance should be referred to Emergence in the first instance. Please contact Emergence:

By phone: +61 2 8280 3000

By email: info@emergenceinsurance.com.au

In writing to: Emergence Complaints, PO Box A2016
Sydney South NSW 1235

If Emergence requires additional information, Emergence will contact **you** to discuss. If **your** complaint is not immediately resolved Emergence will respond within fifteen (15) business days of receipt of **your** complaint or agree a reasonable alternative timeframe to respond.

Step 2

If this does not resolve the matter or **you** are not satisfied with the way a complaint has been dealt with, **you** can contact Lloyd's Underwriters' General Representative in Australia:

By phone: +61 2 8298 0783

By email: idraustralia@lloyds.com

By fax: +61 2 8298 0788

In writing to: Lloyd's Underwriters' General Representative,
Level 9, 1 O'Connell St, Sydney NSW 2000

Lloyd's Underwriters' General Representative in Australia will respond to **your** complaint within fifteen (15) business days of being notified, unless an alternative timetable has been agreed with **you**.

Step 3

If **we** are unable to resolve **your** complaint within 45 calendar days of the date **we** first received **your** complaint or if **you** remain dissatisfied, **you** may seek a free and independent review by the Australian Financial Complaints Authority (AFCA). **We** agree to be bound by AFCA's decisions. **You** do not have to accept their decision and **you** have the right to seek legal advice at any time. **You** can contact AFCA any time:

By visiting: www.afca.org.au

By email: info@afca.org.au

By phone: 1800 931 678 (free call)

In writing to: Australian Financial Complaints Authority,
GPO Box 3, Melbourne VIC 3001

If **your** complaint does not fall within the AFCA Terms of Reference, **you** may be able to refer it to the Financial Ombudsman Service (UK). **We** can provide further details upon request and will do so if **your** complaint reaches this stage.

General Insurance Code of Practice

We proudly support the General Insurance Code of Practice. The objectives of the Code are to:

- commit **us** to high standards of service;
- promote better, more informed relations between **us** and **you**;
- maintain and promote trust and confidence in the general insurance industry;
- provide fair and effective mechanisms for the resolution of complaints and disputes between **us** and **you**; and
- promote continuous improvement of the general insurance industry through education and training.

You can obtain a copy of the Code from the Insurance Council of Australia website www.insurancecouncil.com.au or by phoning [02] 9253 5100.

Privacy Statement

In this Privacy Statement the use of "we", "our" or "us" means the Insurer and Emergence, unless specified otherwise.

We are committed to protecting **your** privacy.

We are bound by the obligations of the *Privacy Act 1988* [Cth] and the Australian Privacy Principles. These set out basic standards relating to the collection, use, storage and disclosure of personal information.

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

The primary purpose for **our** collection and use of **your** personal information is to enable **us** to provide insurance services to **you**.

We may collect personal information in a number of ways, including directly from **you** via **our** website or by telephone or email. Personal information will be obtained from individuals directly where possible and practicable to do so. Sometimes it may be collected indirectly (e.g. from **your** insurance intermediary or co-insureds). If **you** provide personal information for another person **you** represent to **us** that:

- **you** have the authority from them to do so and it is as if they provided it to **us**;

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

We may disclose the personal information **we** collect to third parties who assist **us** in providing the above services, such as related entities, distributors, agents, insurers, reinsurers and service providers. Some of these third parties may be located outside of Australia, including New Zealand, Philippines, Vietnam, Malaysia and United Kingdom. In all instances where personal information may be disclosed to third parties who may be located overseas, **we** will take reasonable measures to ensure that the overseas recipient holds and uses **your** personal information in accordance with the consent provided by **you** and in accordance with **our** obligations under the *Privacy Act 1988* [Cth].

In dealing with **us**, **you** consent to **us** using and disclosing **your** personal information as set out in this statement. This consent remains valid unless **you** alter or revoke it by giving written notice to Emergence's Privacy Officer. However, should **you** choose to withdraw **your** consent, **we** may not be able to provide insurance services to **you**.

The Emergence Privacy Policy, available at www.emergenceinsurance.com.au or by calling Emergence, sets out how:

- Emergence protects **your** personal information;
- **you** may access **your** personal information;
- **you** may correct **your** personal information held by **us**;
- **you** may complain about a breach of the *Privacy Act 1988* [Cth] or Australian Privacy Principles and how Emergence will deal with such a complaint.

If **you** would like additional information about privacy or would like to obtain a copy of **our** Privacy Policy, please contact the Emergence Privacy Officer by:

Postal Address: PO Box A2016, Sydney South NSW 1235
Phone: +61 2 9307 6656
Fax: +61 2 9307 6699
Email: privacyofficer@steadfastagencies.com.au

You can download a copy of the Emergence Privacy Policy by visiting www.emergenceinsurance.com.au

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 on **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 indicated on **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. 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
- b. the net increased costs incurred to avoid a reduction in **revenue** directly as a result of the interruption to **your business** 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.

The amount is calculated by reference to the **records of your business** and any other documents that **we** reasonably request. **Impact on business costs** does not include **cyber event response costs**. **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** and **revenue** 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** reasonable 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 infrastructure** or **IT infrastructure** 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 infrastructure**;
- 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; or
- f. arising out of physical cause or natural peril, such as fire, wind, water, flood, lightning, explosion, collision, subsidence, earthquake, or any other act of God.

The maximum **limit we** will pay 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. **telephone phreaking**; or
- e. **cryptojacking**

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

Section F - Exclusion 19 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**, **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. unintended or unauthorised call charges or bandwidth charges in excess of normal and usual amounts that **you** must pay caused by **telephone phreaking**, or
- c. unintended or unauthorised bandwidth charges and electricity costs in excess of normal and usual amounts that **you** must pay caused by **cryptojacking**.

investigation costs means costs **you** incur with **our** prior consent, not unreasonably withheld, 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.

You must report the **cyber theft, socially engineered theft, identity-based theft, telephone phreaking or cryptojacking** to, respectively, the Australian Cyber Security Centre, **your** financial institution and **your** telephone service provider, within 24 hours of it first being discovered by **you**.

The sublimit for any claim or series of related claims for **socially engineered theft** is stated in **your schedule**. The maximum **limit** **we** will pay for all **direct financial loss** under this Optional Cover - Criminal Financial Loss is stated 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 21 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 events, losses, claims, preventative shutdown allowance, 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**.

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

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**.

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

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

- **crimeware** which is any malware of any type intentionally designed to cause harm to **your IT infrastructure** but does not include **cyber espionage** or **point of sale intrusion**.
- **cyber espionage** which is unauthorised access to an item of **your IT infrastructure** 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 infrastructure**, or data in **your IT infrastructure**, 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 infrastructure**. This includes a distributed **denial of service**.
 - **hacking** which is malicious or unauthorised access to **your IT infrastructure**.
 - **insider and privilege misuse** which is unapproved or malicious use of **your IT infrastructure** by **your** employees, outsiders in collusion with **your** employees, or business partners who are granted privilege access to **your IT infrastructure** but does not include theft, **socially engineered theft**, **identity-based theft** or **cyber theft**.
 - **miscellaneous errors** where unintentional actions directly compromise a security attribute of an item of **your IT infrastructure** 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 infrastructure** that reads data from a payment card.
 - **physical theft and loss** where an item of **your IT infrastructure** 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 Infrastructure** 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 infrastructure**, 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 or programs in **your IT infrastructure** 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.
 - **data securing costs** incurred in securing **your IT infrastructure** 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 infrastructure**.
 - **identity theft response costs** incurred in supporting an individual with reporting of the **identity theft** and re-establishing identity and essential records.

- **notification costs** incurred in notifying any person whose data or information has been accessed or lost including the cost of preparing a statement to the Office of the Australian Information Commissioner or other authorities.
- **public relations costs** incurred in responding to a **cyber event** 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 infrastructure**.

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 infrastructure** and without **your** knowledge. **Cyber theft** does not include **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**.

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.

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** and is exclusive of GST.

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

impact on business costs means:

- 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
- the net increased costs incurred 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** reasonably 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**.

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

IT contractor is a third party contracted to provide, maintain or manage IT infrastructure.

IT infrastructure means all of the hardware, firmware, software, networks, facilities, and the like, owned by or leased to, rented to or licensed to **you**, irrespective of where these are hosted, insofar as they are required to develop, test, deliver, monitor, control or support IT services used in **your business**. The term **IT infrastructure** 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. non-conformance with any legal requirement relating to web access such as the Disability Discrimination Act of 1992; or
- e. 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 infrastructure** in response to a **cyber event** in **your business**, or a credible threat to **your IT infrastructure** following:

- a. a **cyber event** at **your** direct customer, supplier or business partner,
- b. specific instruction from **your** financial institution, law enforcement or the Australian Signals Directorate 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**

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 infrastructure**.

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
- 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 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 **your IT infrastructure**.

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 reasonably 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 infrastructure**; or
- b. the safe resumption of operations of your **IT infrastructure**.

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.

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 infrastructure**, having believed such facts to be genuine and true. **Socially engineered theft** does not include **cyber theft** or **identity-based theft**.

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 **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 **cyber events, losses or claims** prior to you acquiring it;
- e. the entity's **IT infrastructure** and risk management are equal to or better than yours, or you will use best endeavours either to bring its **IT infrastructure** and risk management to an equivalent standard or to ensure its **IT infrastructure** will be absorbed promptly into your **IT infrastructure**.

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.

we/our/us means certain underwriters at Lloyd's (the underwriters), the insurer 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 **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

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

We will not pay any **impact on business costs, loss, cyber event response costs 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 contractors** or external suppliers.
6. arising from, or resulting in, or causing an **employment wrongful act**.
7. for an action brought against **your** directors or officers acting in that capacity or an action against **you** for an error or omission while acting in a professional or fiduciary capacity or an action against **you** for providing services to others as an **IT contractor**.
8. in connection with any products, hardware, software, software as a service, platform as a service, infrastructure as a service, or related services or IT infrastructure **you** sell, lease, license or otherwise provide to others for a fee.
9. 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.
10. arising from, attributable to, or as a consequence of pollution.
11. 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.
12. arising from any physical act of war, invasion or warlike operation, civil war, riot, civil commotion, rebellion, revolution, insurrection or civil uprising.
13. 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.
14. arising from, attributable to, or in consequence of any electromagnetic field, electromagnetic radiation or electromagnetism.
15. 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**.
16. that is related to damages characterised or described as aggravated, punitive or exemplary damages.
17. caused by defective equipment, ordinary wear or deterioration, faulty design or construction or insufficient capacity of **your IT infrastructure**.
18. arising out of or caused by outage of a **utility provider**.
19. arising from, attributable to, or as a consequence of **cyber theft, socially engineered theft, identity-based 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, telephone phreaking or cryptojacking**.
20. 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.
21. arising from, attributable to, or as a consequence of any joint venture or consortium in which **you** have an interest.
22. 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**.
23. 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.
24. directly or indirectly involving any actual or alleged infringement of any patent.

Section G – Claims Conditions

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

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

- 1. You** must immediately ring the Emergence **cyber event** reporting line on 1300 799 562 or notify Emergence in writing at claims@emergenceinsurance.com.au and provide details and circumstances of the event, including any **claims**, demands or notices received by **you** or proceedings against **you**.
- 2. You** must report **cyber theft, socially engineered theft, identity-based theft, telephone phreaking or cryptojacking** to, respectively, the Australian 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** determine 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**. **Our** consent will not be unreasonably withheld.
- 12. Defence costs** must be approved by **us** before they can be incurred by **you**. **We** will not unreasonably withhold **our** consent to **you** incurring reasonable and necessary **defence 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** or **claim** and some of that cost is not **impact on business costs, 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 or identity-based 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**.

If **you** do not comply with the following General Conditions, **we** may refuse to pay a claim in whole or in part or in some circumstances in accordance with the law cancel the **policy**.

1. **You** must notify **us** in writing as soon as practicable of any change in **your business activity**.
2. Subject to **your** rights under the *Insurance Contracts Act 1984* [Cth], **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**.
3. **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.
4. 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.
5. This **policy** and any rights under it cannot be assigned without **our** written consent.
6. GST, Goods & Services Tax and Input Tax Credit have the meanings attributed to them under the *A New Tax System (Goods and Services Tax) Act 1999* [Cth]. No payment will be made to **you** for any GST

liability in connection with a covered claim. It is **your** responsibility to inform **us** whether **you** are entitled to an Input Tax Credit for any amounts claimed under this **policy**. The **excess** and all **policy limits** stated on **your schedule** are exclusive of GST.

7. **You** may cancel the **policy** in accordance with **your** 'cooling off rights' within the first 14 days from commencement.

After this 14 day period **you** may cancel the **policy** at any time by providing **us** with written notice stating when thereafter cancellation is to take effect. As long as no claim has been made and there has been no **cyber event**, **we** will refund premium to **you** calculated on a pro rata basis less any non-refundable government taxes, charges or levies, and less an administrative charge of \$110 inclusive of applicable GST.

We can only cancel the **policy** in accordance with the provisions of the *Insurance Contracts Act 1984* [Cth].
8. **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.
9. 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. The proceeds of any subrogation or recovery action will be applied between **you** and **us** in accordance with the provisions of the *Insurance Contracts Act 1984* [Cth].
10. 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 subject only to the terms and conditions of this **policy**, cover under this **policy** shall apply in excess of such other insurance. **You** are required to provide **us** details of the other insurance.
11. **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.

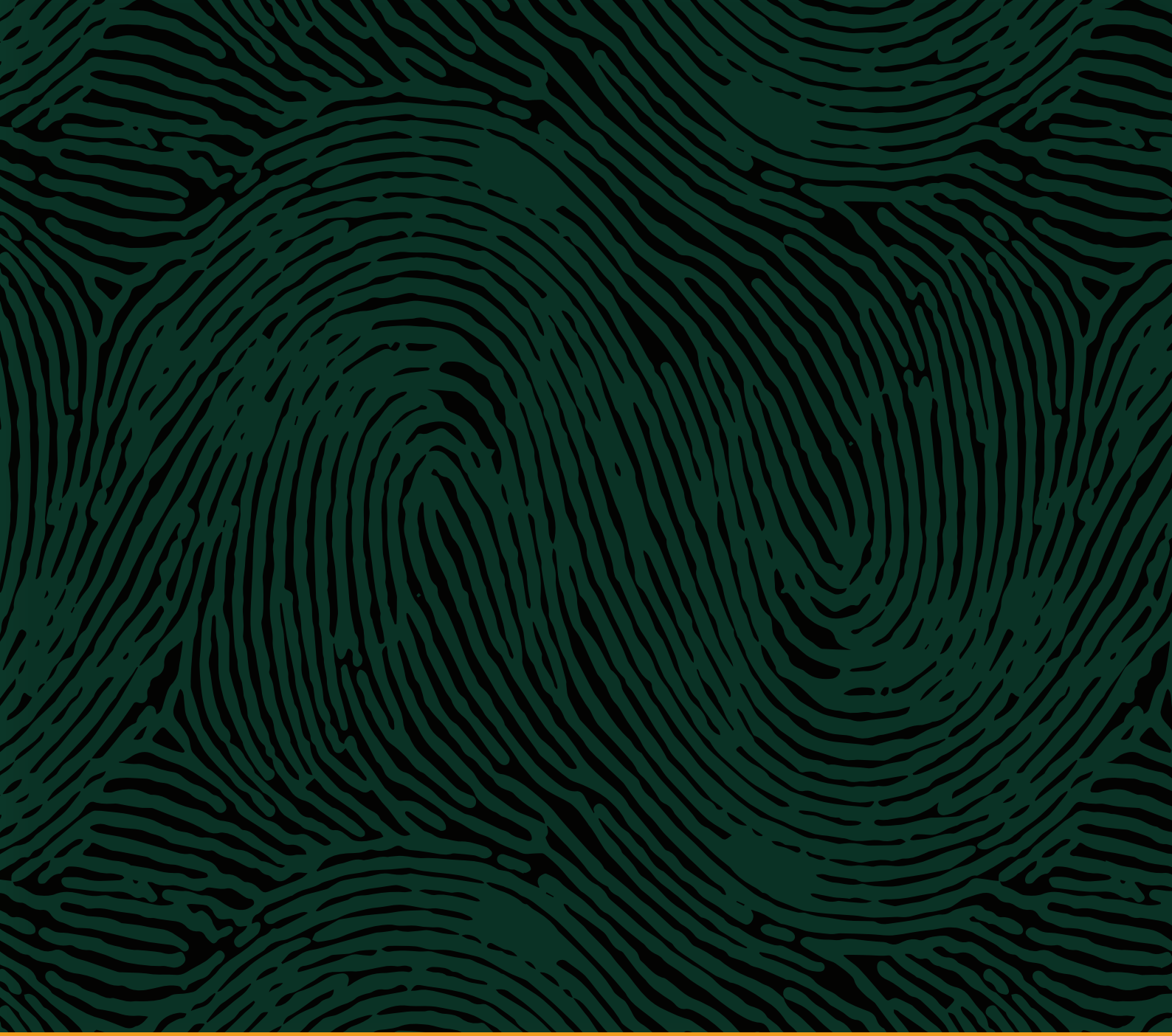
12. All premiums, **limits**, **loss** and other amounts under this **policy** are expressed and payable in Australian dollars. Except as otherwise provided, if judgement is rendered, settlement is denominated or another element of loss under this **policy** is stated in other than Australian dollars, payment under this **policy** shall be made in Australian dollars at the cash rate of exchange for the purchase of Australian dollars in accordance with the Reserve Bank of Australia on the date final judgement is reached, the amount of the settlement is agreed upon or the other element of **loss** becomes due.
13. If **you** report a **cyber event** 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 **cyber event** happened.
14. All reported incidents and claims which arise out of one **cyber event** or a series of **cyber events** involving **your IT infrastructure** or **business** will be deemed to be one **cyber event** and only one **aggregate** will apply.
15. 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.
16. Where **you**:
- prior to the **policy period** first became aware of facts or circumstances that might give rise to a **claim**; and
 - did not notify **us** of such facts or circumstances prior to the **policy period**; and
 - 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**.
17. 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.
18. The insurers accepting this insurance agree that:
- if a dispute arises under this insurance, this **policy** will be subject to Australian law and practice and the insurers will submit to the jurisdiction of any competent Court in the Commonwealth of Australia;
 - any summons notice or process to be served upon the insurers may be served upon:

Lloyd's Underwriters' General Representative in Australia Level 9, 1 O'Connell Street
Sydney NSW 2000

who has authority to accept service and to appear on the insurers' behalf;
 - 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.
- In the event of a claim arising under this **policy** NOTICE should be given to Emergence Pty Ltd as soon as possible.
19. 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.

This work is copyright. Apart from any use permitted under the Copyright Act 1968 (Cth), no part may be reproduced by any process, nor may any other exclusive right be exercised without the permission of the publisher.

© Emergence Insurance Pty Ltd 2021



emergence

Level 4, 99 Bathurst Street, Sydney NSW 2000
[02] 8280 3000
emergenceinsurance.com.au