BUSINESS CYBER INSURANCE

emergence

cyber event protection

CEP-005 AUS IMPORTANT INFORMATION AND POLICY WORDING

BUSINESS CYBER INSURANCE

emergence

cyber event protection

CEP-005
Important Information & Policy Wording

Emergence is your award-winning underwriting agency solely focused on providing flexible, innovative insurance solutions to help protect businesses against cyber risks.

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 Emergence by Lloyd's underwriters to administer and issue policies, alterations, and renewals. In all aspects of arranging this **policy**, Emergence acts as an agent for underwriters and not for **you**.

Contact details are:

Email: info@emergenceinsurance.com.au
Telephone: 1300 799 562
Postal address: GPO Box R748
Royal Exchange
Sydney NSW 2001

About Our Services

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

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

All of the services are designed to enhance **your** cyber security while **you** remain a **policyholder** with Emergence.

We will also provide advice to **you** after a claim on how best to secure **your IT**.

Our Cyber Breach Coach Service

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

See: How to notify **us** if a **cyber event** happens, below.

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, push payment 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.

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.

Section F – Exclusions

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

*Note: **You** should read these exclusions carefully and speak to **your** insurance broker about what this **policy** covers and what other insurance 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**, **multimedia injury** or **Payment Card Industry liability** 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

The **policy** documents will be sent electronically to **your** insurance broker's email address.

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 in 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 also charges a **policy** fee in addition to the premium, as indicated on the **schedule**.

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.

Complaints and Dispute Resolution Process

If **you** have any concerns or wish to make a complaint in relation to this **policy** or **our** services, please let **us** know and **we** will attempt to resolve **your** concerns in accordance with **our** Internal Dispute Resolution procedure. Please contact Emergence in the first instance:

Complaints Officer, Emergence Insurance Pty Ltd
By Phone: 1300 799 562
By Email: info@emergenceinsurance.com.au
By Post: Emergence Complaints,
GPO Box R748
Royal Exchange
Sydney NSW 2001

We will acknowledge receipt of **your** complaint and do **our** utmost to resolve the complaint to **your** satisfaction within ten (10) business days.

If **we** cannot resolve **your** complaint to **your** satisfaction, **we** will escalate **your** matter to Lloyd's Australia who will determine whether it will be reviewed by their office or the Lloyd's UK Complaints team. Lloyd's contact details are:

Lloyd's Australia Limited
By Phone: +61 2 8298 0783
By Email: idraustralia@lloyds.com
By Post: Suite 1603 Level 16,
1 Macquarie Place, Sydney NSW 2000

A final decision will be provided to **you** within thirty (30) calendar days of the date on which **you** first made the complaint unless certain exceptions apply.

You may refer **your** complaint to the Australian Financial Complaints Authority ('AFCA'), if **your** complaint is not resolved to **your** satisfaction within thirty (30) calendar days of the date on which **you** first made the complaint or at any time. AFCA can be contacted as follows:

By Phone: 1800 931 678
By Email: info@afca.org.au
By Post: GPO Box 3, Melbourne VIC 3001
Website: www.afca.org.au

Your complaint must be referred to AFCA within two (2) years of the final decision, unless AFCA considers special circumstances apply. If **your** complaint is not eligible for consideration by AFCA, **you** may be referred to the Financial Ombudsman Service (UK) or **you** can seek independent legal advice. **You** can also access any other external dispute resolution or other options that may be available to **you**.

General Insurance Code of Practice

The Insurance Council of Australia Limited has developed the General Insurance Code of Practice ("the Code"), which is a voluntary self-regulatory code. The Code aims to raise the standards of practice and service in the insurance industry.

Lloyd's has adopted the Code on terms agreed with the Insurance Council of Australia. For further information on the Code please visit www.codeofpractice.com.au

The Code Governance Committee (CGC) is an independent body that monitors and enforces insurers' compliance with the Code. For more information on the Code Governance Committee (CGC) go to www.insurancecode.org.au

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 the 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:

By Post: GPO Box R748
Royal Exchange
Sydney NSW 2001
By Phone: 1300 799 562
By Email: privacyofficer@emergenceinsurance.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

1. cyber event in your business

If a **cyber event** or **system failure** happens at or within **your business** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** the **impact on business costs**.

The maximum **we** will pay in any one **policy period** for **system failure** under Section A is as stated in the **schedule**.

2. cyber event in your IT contractor's business

If a **cyber event** or **system failure** happens at or within **your IT contractor's** business, which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** the **impact on business costs**.

The maximum **we** will pay in any one **policy period** for **system failure** under Section A is as stated in the **schedule**.

3. preventative shutdown

If a **preventative shutdown** happens during the **policy period** which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **you** a **preventative shutdown allowance**.

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

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:

1. a **cyber event**, or
2. **multimedia injury,** or
3. **Payment Card Industry liability**

at or within **your business**.

Section C – Cyber Event Response Costs

1. cyber event in your business

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

2. cyber event in your IT contractor's business

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

3. cyber event in your data processor's business

If there is a **cyber event** at or within **your data processor's** business which is first discovered by **you** and notified to **us** during the **policy period**, then **we** will pay **your data processor 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 and conditions of the **policy** unless otherwise stated in the Optional Cover.

The 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 sublimits form part of and are included within the **aggregate**.

Optional Cover – Non-IT Contingent Business Interruption and System Failure Cover

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

a. **supplier outage**, or

b. **supplier system failure**.

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

cyber event is extended to be a **cyber event** at or within the business of a **supplier**. For the purposes of this cover only, it shall not include a **cyber event** which happens at or within **your business**, or at or within an **IT contractor'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 **supplier 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 a **supplier outage** or a **supplier system failure** 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.

Impact on business costs does 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 any **impact on business costs** incurred under this Optional Cover – Non-IT Contingent Business Interruption and System Failure 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 supply from **your supplier** resumes, or until **you** have a substitute supply, plus reasonable additional time to allow **your business** to normalise. The **indemnity period** shall not exceed a total length of 35 days unless stated otherwise in **your schedule**.

supplier means a direct external supplier of goods or services to **your business** other than a **utility provider** or an **IT contractor.**

supplier IT means information technology used at or within **your supplier's** business.

supplier outage means an interruption to **your business** directly arising from an outage at **your supplier** where, in **our** reasonable opinion, the outage has been caused by a **cyber event** at or within the business of such **supplier**.

supplier system failure means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **your supplier's IT** 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 the **supplier IT**;

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;

f. arising out of **your IT** or **IT** under the direct operational control of **your IT contractor**.

The maximum **we** will pay for all **supplier outage** and all **supplier system failure** in any one **policy period** under this Optional Cover – Non-IT Contingent Business Interruption and System Failure is stated in **your schedule**. The sublimit is included in, forms a part of, and is not in addition to the **aggregate**.

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 15 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, 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 sublimit for Optional Cover – Criminal Financial Loss.

You must report the **cyber theft, socially engineered theft, identity-based theft, push payment 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 maximum sublimit **we** will pay in any one **policy period** for all **direct financial loss** under this Optional Cover - Criminal Financial Loss 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**.

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

Optional Cover – D&O Liability Cover

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

For the purpose of this Optional Cover – D&O Liability Cover only the words listed below have been given a specific meaning and the specific meanings apply:

claim means any written demand, notice of pending action or civil, criminal, administrative, regulatory or arbitral proceedings against **your** directors or officers seeking compensation or other legal remedy caused by or in connection with a **cyber wrongful act**.

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

Section F - Exclusion 23 a. of the **policy** is varied to the extent that cover is provided under this Optional Cover – D&O Liability Cover.

The following additional exclusion applies to this Optional Cover – D&O Liability Cover only:

We will not pay a **loss** that **you** are legally liable for arising out of, attributable to, or as a consequence of a **claim** under this Optional Cover – D&O Liability Cover:

a. if **you** are listed on the Australian Stock Exchange, if **your** shares are traded on any other exchange, or pursuant to any actual or proposed initial or subsequent public offering.

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

If any **claim** arises under this Optional Cover 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 Optional Cover shall apply in excess of such other insurance. **You** are required to provide **us** details of the other insurance.

The maximum sublimit **we** will pay in any one **policy period** for all **claims** under this Optional Cover – D&O Liability Cover is stated in **your schedule**. The sublimit for this Optional Cover - D&O Liability Cover forms part of, and is not in addition to, the **limit** for Section B – Loss to Others.

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 at or within **your business** 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.** The sublimit for Tangible Property Cover forms part of, and is not in addition to, the **limit** for Section C - 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 16 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 insureds, under Section 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 sublimits 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 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**, **multimedia injury** or **Payment Card Industry liability**.

computer system, for the 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 means any of the following:

- **crimeware** which is any malware of any type intentionally designed which causes harm to **IT** but does not include **cyber espionage** or **point of sale intrusion**.
- **cyber espionage** which is unauthorised access to an item of **IT** linked to a state affiliated or criminal source exhibiting the motive of espionage.
- **cyber extortion** which is a crime involving ransomware or an attack or threat of attack against **IT**, or data in **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 **IT**. This includes a distributed **denial of service**.
- **hacking** which is malicious or unauthorised access to **IT**.
- **insider and privilege misuse** which is unapproved or malicious use of **IT** by **your** employees, outsiders in collusion with **your** employees, or business partners who are granted privileged access to **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 **IT** but does not include theft, **socially engineered theft** or **cyber theft.**
- **payment card skimming** involving a skimming device being physically implanted through tampering into an item of **IT** that reads data from a payment card.
- **physical theft and loss** where an item of **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 **IT** where retail transactions are conducted, specifically where purchases are made by a payment card.
- **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, data restoration costs,** or **identity theft response costs.**
- **web app attacks** where a web application was the target of attack against **IT**, including exploits of code level vulnerabilities in the application.

cyber event response costs means the reasonable and necessary costs and expenses **you** incur with **our** agreement and consent, which will not be unreasonably withheld, 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 **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 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 **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 **IT** and 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 following the **identity theft**.
- **IT forensic costs** incurred by **you** with **our** prior consent, to investigate a **cyber event** or suspected **cyber event**.
- **legal advice costs** 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 preparing a statement to the Office of the Australian Information Commissioner or other authorities.
- **public relations costs** incurred in responding to a **cyber event**, or adverse media arising from a **cyber event**, including external public relations, media, social media and communications management to prevent reputational harm to **you**.
- **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 **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**.

data processor means a person other than an **IT contractor** who processes **your** data under a contract with **you**.

data processor response costs means the reasonable and necessary costs and expenses **you** incur in responding to a **cyber event** at or within **your data processor's** business that impacts **your** data being:

- **credit and identity monitoring costs,**
- **cyber extortion costs,**
- **data restoration costs,**
- **data securing costs,**
- **external management costs,**
- **identity theft response costs,**
- **legal advice costs,**
- **notification costs and**
- **public relations costs.**

data processor response costs does not mean the **data processor's** own costs.

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** or **system failure** 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** and is exclusive of GST. If there is more than one **excess** stated in **your schedule** then **you** will pay the higher **excess** if the incident or claim relates to that higher **excess.**

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**.

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**.

impact on business costs means:

a. the amount that the **revenue you** earn during the **indemnity period** falls short of the **revenue you** ordinarily earn directly as a result of a **cyber event** or **system failure**, less any consequent savings, and less any **delayed revenue**, plus

b. the net increased costs incurred during the **indemnity period** to avoid a reduction in **revenue** directly as a result of a **cyber event** or **system failure** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **revenue** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries or overhead expenses.

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

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

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 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 first discovery of the **cyber event** or **system failure** until the **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 means all of the hardware, servers, systems, firmware, software, networks, platforms, facilities owned by, leased to, rented to or licensed to:

a. **you**, or

b. **your IT contractor**

insofar and solely as they are required to develop, test, deliver, monitor, control or support information technology services **you** use in **your business**.

The term **IT** includes all of the information technology, but not the associated people, processes and documentation.

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

IT contractor response costs means the reasonable and necessary costs and expenses **you** incur in responding to a **cyber event** at or within **your IT contractor's** business that impacts **your** data being:

- **credit and identity monitoring costs,**
- **cyber extortion costs,**
- **data restoration costs,**
- **data securing costs,**
- **external management costs,**
- **identity theft response costs,**
- **legal advice costs,**
- **notification costs and**
- **public relations costs.**

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

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** or **system failure**, irrespective of the number of claim(s). The 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 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** in response to a **cyber event** at or within **your business**, or a credible threat to **your IT** following:

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

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**.

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 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 **IT**.

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

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

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

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

c. the expiration of the 48 consecutive hours.

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 at or within **your business** 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 the 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** 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** 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 **IT**.

system failure means an interruption to **your business** directly arising from an unintentional, unexpected and unplanned outage of **IT**, 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 **IT**;

d. falling within parameters of a service level agreement;

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

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

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, stock exchanges, security exchanges, 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 this **policy** and Emergence acting on behalf of underwriters as the issuer of this **policy**.

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

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

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 arising from attributable to or as a consequence of:

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

2. 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. any **cyber event**, **system failure**, **multimedia injury**, loss, fact or circumstance known to **you** or discovered by **you** before the **policy period**.

4. 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. **your** bankruptcy, liquidation or insolvency or the bankruptcy, liquidation or insolvency of any **IT contractors** or external suppliers.

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

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

   b. pollution,

   c. any electromagnetic field, electromagnetic radiation or electromagnetism.

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

9. or 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. or directly or indirectly occasioned by or happening through,

    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 **us** 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. 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. a liability 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**.

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

14. or caused by outage, failure or malfunction of a **utility provider**.

15. **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**.

16. any joint venture or consortium in which **you** have an interest.

17. or 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**.

18. any **claim, loss**, judgement or award made in the United States of America or which applied the laws of the United States of America.

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

20. 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.

21. or 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.

22. 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.

Exclusions – policy Section B only

The following exclusions apply to Section B only.

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

23. for an action:

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

    b. brought against **you** as a result of any failure of information technology services provided, maintained, serviced or managed by **you** for a third party for a fee as part of **your business activities**.

24. in connection with any products, including packaging, labelling or instructions, that **you** design, assemble, manufacture, distribute, service, sell, rent, lease or license to others for a fee.

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** or **system failure**, 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, push payment 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** in determining if there is a **cyber event** or **system failure** 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 any reasonable requests made by **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** 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** and **you** are actively pursuing the recovery of the funds through **your** financial institution **we** will pay the claim within 30 days of the claim being notified to **us**. **You** must cooperate with and assist **us** in **our** attempts to recover **your direct financial loss** and **you** must reimburse **us** for any funds recovered by **you.**

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 cancel the **policy** to the extent permitted by law.

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. if **you** become aware of a pending appointment of a receiver or the commencement of bankruptcy or winding up proceedings to **your business**; or
    c. if **you** form or acquire an entity that does not meet the criteria for automatic inclusion under this **policy** as set forth in the definition of **subsidiary**.
3. **You** must maintain IT security practices and procedures to a standard equal or better than **you** had in place at the time this **policy** commenced. A failure to adhere to such practices and procedures by an employee or an external supplier 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**, **system failure, multimedia injury, Payment Card Industry liability** 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** 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 have been no circumstances that might lead to a **claim**, **cyber event** or **system failure**, **we** will refund premium to **you** calculated on a pro rata basis less any non-refundable government taxes, charges or levies.

    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 to the extent permitted by law. **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, 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.
14. All reported incidents and claims which arise out of one **cyber event** or **system failure**, or a series of **cyber events** or **system failures** will be deemed to be one **cyber event** or **system failure** 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**:

    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**.

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 a **cyber event**, **multimedia injury** or **Payment Card Industry liability** that happened prior to termination.

18. The insurers accepting this insurance agree that:

    a. 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;

    b. any summons notice or process to be served upon the insurers may be served upon:

    Lloyd's Australia Limited
    Suite 1603 Level 16, 1 Macquarie Place
    Sydney NSW 2000

    who has authority to accept service and to appear on the insurers' behalf;

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

    In the event of a claim arising under this **policy** NOTICE should be given to Emergence Insurance 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.

20. Sanctions Limitation Clause

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

Level 3, Bligh House 4-6 Bligh Street,
Sydney NSW 2000

1300 799 562

emergenceinsurance.com.au

AUSTRALIA'S AWARD-WINNING UNDERWRITING AGENCY

emergence