emergence

Cyber Enterprise Solution

CES-002.a
General Information
& Policy Wording

Contents

emergence

Cyber Enterprise Solution CES-002.a
Important Information & Policy Wording

Published June 2023

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 Emergence Insurance Pty Limited

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

Email: info@emergenceinsurance.com.au
Telephone: +61 1 300 799 562
Postal address: GPO Box 327 Sydney, NSW 2001

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.

Claims Made Notice

Section C – Cyber & Privacy Liability and Section F – Optional Cover – Multimedia Liability Cover of this policy are issued on a 'claims made and notified' basis. This means that Section C – Cyber & Privacy Liability and Section F – Optional Cover – Multimedia Liability Cover respond to:

a. **Claims** or **multimedia 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** or **multimedia claim** may be made against **you**; and

b. written notifications 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** or **multimedia claim** against **you** even if a **claim** or **multimedia claim** has not yet been made against **you**. If **you** decide to notify any such facts, 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 to any claim or **multimedia claim** against **you** arising from those facts, even if the claim or **multimedia claim** is not made against **you** until after the **policy** has expired. When the **policy period** expires, no new notification of facts can be made to **us** under 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 policy** 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 **policy** as if it never existed.

Headings

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

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 327 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

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**, of the types of third parties **we** may provide it to, of 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 to **us**.

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, the EU 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:

Post: GPO Box 327 Sydney, NSW 2001
Phone: +61 1 300 799 562
Email: privacyofficer@emergenceinsurance.com.au

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

Policy Wording

Preamble

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-E, and for any Optional Covers selected. The **aggregate** is the most **we** will pay for all Sections, including Extensions and any Optional Covers. The **limit** stated on **your schedule** is exclusive of GST.

Section A – Business Interruption

If a **cyber event** happens in **your** business, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, and that **cyber event** causes a **system outage**, 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 – Dependent Business Interruption

If a **cyber event** happens to **your IT contractor**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, that causes a **system outage** in **your business**, then **we** will pay **you** the **impact on business costs**.

Section C – Cyber & Privacy Liability

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** if that **claim** was made against **you** because of a **cyber event** in **your business**.

Section D – Cyber Event Response Costs

If there is a **cyber event** in **your business**, or a **cyber event** to **your IT contractor**, which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then we will pay **your cyber event response costs**.

Section E – Extensions

1. emergence cyber breach coach

If there is, or **you** reasonably suspect there is, a **cyber event** in **your business**, which is first discovered by **your senior management team** 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 the emergence cyber breach coach does not form part of **cyber event response costs**, does not erode the **aggregate** and no **excess** applies.

2. betterment costs

If there is a **cyber event** in **your business** which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then **we** will pay the additional cost and expenses to replace or restore **your** software with newer, upgraded, and/or improved versions of the impacted software.

The maximum **limit we** will pay is 20% more than the cost would have been to repair or replace the original version of the software, or the **limit** stated in **your schedule**, whichever is the lesser.

3. claims preparation costs

We will pay up to the maximum **limit** stated in **your schedule** for claims preparation costs incurred with **our** prior written consent for a third party to assist **you** to verify **impact on business costs** incurred by **you**.

4. pursuit costs

We will pay up to the maximum **limit** stated in **your schedule** for pursuit costs incurred with **our** prior written consent as reward to a third party (other than a law enforcement officer, **your** current or former employee, or **your IT contractor**) for assistance leading to the arrest and conviction of the perpetrator of a **cyber event** leading to a claim by **you** which is covered under this **policy**.

5. telephone phreaking

We will pay unintended or unauthorised call charges or bandwidth charges, in excess of **your** normal and usual amounts, that **you** must pay caused by **telephone phreaking** that is first discovered by **your senior management team** and notified to **us** during the **policy period**.

6. cryptojacking

We will pay unintended or unauthorised bandwidth charges and electricity costs in excess of **your** normal and usual amounts, that **you** must pay caused by **cryptojacking** that is first discovered by **your senior management team** and notified to **us** during the **policy period**.

Section F – 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** and is the maximum **we** will pay in any one **policy period** for all claims under that optional cover. Optional cover **limits** form part of and are included within the **aggregate**.

1. optional cover – reputational harm cover

If an **adverse media event** happens involving **your business** which is first discovered by **your senior management team** and notified to **us** during the **policy period**, then **we** will pay **you** the **reputational harm impact**.

2. optional cover – system failure cover

We will pay **you impact on business costs** caused by **system failure**.

For the purpose of this optional cover – system failure only, the words listed below have been given a specific meaning and the specific meanings apply:

indemnity period is amended and means the continuous period starting from the first interruption to **your business** until **your IT infrastructure** is sufficiently restored to support **your** usual **business** operations, however the **indemnity period** shall be the shorter of 90 days or the period shown in **your schedule**.

3. optional cover – multimedia liability cover

We will pay a **loss** that **you** are legally liable for arising out of a **multimedia claim** that is first made against **you** and notified to **us** during the **policy period** because of **multimedia injury**.

Section H – Exclusion 11 of the **policy** is not applicable to any **claim** under the **policy** pursuant to this optional cover – multimedia liability cover.

4. optional cover – tangible property cover

We will pay the cost of the replacement or repair of **your** IT hardware that is 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**, provided that replacing or repairing **your** IT hardware is more cost effective than installing new firmware or software onto **your** existing IT hardware.

We will not pay any cost to replace or repair:

a. IT hardware that is physically stolen, lost, or damaged;

b. servers; or

c. **operational technology**;

under this optional cover.

Section H – Exclusion 1 of the **policy** is not applicable to any **claim** under the **policy** pursuant to this optional cover – tangible property cover.

5. optional cover – JV and consortium cover

The cover provided under Section C – Cyber & Privacy Liability 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 H – Exclusion 20 of the **policy** is not applicable to any **claim** under the **policy** pursuant to this optional cover – joint venture and consortium cover.

Section G – Definitions

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

1. **act(s) of terrorism** means 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.

2. **adverse media event** means any negative publication(s), including print, television, radio, and social media, in relation to a covered **cyber event** in **your business**.

3. **aggregate** means the most **we** will pay under this **policy**, including **defence costs**, in any one **policy period** for all **cyber events**, **system failures**, **losses**, **claims**, **multimedia claim**s, **preventative shutdown allowance**, or **direct financial loss** for all **insureds**, under Sections A-E and any Optional Covers taken out by **you**. All **limits** and sublimits are included in and form part of the **aggregate**. The **aggregate** is stated in **your schedule**.

4. **business** means the **policyholder's business** set out in **your schedule**.

5. **claim** means any written demand, notice of pending action or civil, criminal, administrative, regulatory, or arbitral proceedings against **you** by a third party seeking compensation or other legal remedy as a consequence of or in connection with a **cyber event**. **Claim** does not include a **multimedia claim**.

6. **computer system** means any computer, hardware, software, communications system, electronic device (including but not limited to, smart phone, laptop, tablet, wearable device), server, cloud infrastructure or microcontroller including any similar system or any configuration of the aforementioned and including any associated input, output, data storage device, networking equipment or back up facility. This definition applies to exclusion 10 only.

7. **computer systems** means **your IT infrastructure** and **operational technology**.

8. **cryptojacking** means the unauthorised use of **your computer systems** by a third party to mine digital currency that causes **you direct financial loss**.

9. **cyber event** means any of the following:

    a. **crimeware** which is any malware of any type intentionally designed to cause harm to **your computer systems** but does not include **cyber espionage** or **point of sale intrusion**.

    b. **cyber espionage** which is unauthorised access to an item of **your computer systems** linked to a state affiliated or criminal source exhibiting the motive of espionage.

    c. **cyber extortion** which is a crime involving an attack or threat of attack against **your computer systems**, or data in **your computer systems**, coupled with a demand for money or other valuable consideration (including digital currency) to avert or stop the attack.

    d. **denial of service** which is intended to uniquely compromise the availability of **your computer systems**. This includes a distributed **denial of service**.

    e. **hacking** which is malicious or unauthorised access to **your computer systems**.

    f. **insider and privilege misuse** which is unapproved or malicious use of **your computer systems** by **your** employees, outsiders in collusion with **your** employees, or business partners who are granted privilege access to **your computer systems** and which directly compromises a security attribute of an item of **your computer systems**, or leads to unauthorised access to, unauthorised disclosure of or loss of **your** data, or data **you** hold on behalf of third parties in connection with the **business**, (including non-electronic data).

    g. **miscellaneous errors** which is where unintentional action(s) directly compromise(s) a security attribute of an item of **your computer systems**.

    h. **privacy error** which is where unintentional act(s) or omission(s) by **your** employee(s) or **your IT contractor(s)** lead(s) to unauthorised access to, unauthorised disclosure of or loss of **your** data or data **you** hold on behalf of third parties in connection with the **business** (including non-electronic data).

    i. **payment card skimming** which is where a skimming device is physically implanted through tampering into an item of **your IT infrastructure** and that skimming device reads data from a payment card.

    j. **physical theft and loss** which is 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.

    k. **point of sale intrusion** which is a remote attack against **your computer systems** where retail transaction purchases are made by a payment card.

    l. **web app attacks** which is where a web application was the target of an attack against **your IT infrastructure**, including exploits of code level vulnerabilities in the application.

10. **cyber event response costs** means the following reasonable costs and expenses:

    a. **credit and identity monitoring costs** which means costs, reasonably incurred by **you** with **our** prior consent, to engage monitoring services by a third party for persons affected by a **cyber event** for a period of up to 12 months.

    b. **crisis management costs** which means costs, reasonably incurred by **you** with **our** prior consent, to respond to a **cyber event** when that response is reasonably necessary to counter a credible impending threat to stage a **cyber event** against **your computer systems**.

    c. **cyber extortion costs** which means costs, reasonably incurred by **you** with **our** prior consent, to respond to a **cyber event** where a third party is seeking to obtain pecuniary gain from **you** through **cyber extortion**.

d. **data restoration costs** which means costs, reasonably incurred by **you** with **our** prior consent, to:

   i. restore or replace **your** data or programs in **your computer systems** that have been lost, damaged, or destroyed;

   ii. mitigate or prevent further damage; and

   iii. purchase replacement licenses, if necessary.

   Data restoration costs does not include any costs to redesign, replicate or reconstitute proprietary information, facts, concepts, or designs.

e. **data securing costs** which means costs, reasonably incurred by **you** with **our** prior consent, to secure **your computer systems** to avoid ongoing **impact on business costs, loss**, and **cyber event response costs**.

f. **identity theft response costs** which means costs, reasonably incurred by **you** with **our** prior consent, to support an individual with reporting of the **identity theft** and re-establishing identity and essential records.

g. **IT forensic costs** which means costs, reasonably incurred by **you** with **our** prior consent, to investigate and determine the cause and scope of a **cyber event**.

h. **legal costs** which means costs, reasonably incurred by **you** with **our** prior consent, to retain legal or regulatory advice in relation to **your** rights and obligations in respect of any legal and regulatory issues that arise as a result of a **cyber event**.

i. **notification costs** which means costs, reasonably incurred by **you** with **our** prior consent, to notify 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.

j. **PCI Investigation costs** which means costs, reasonably incurred by **you** with **our** prior consent, to appoint an auditor to investigate any **payment card industry liability** that arises out of a **cyber event**.

k. **public relations costs** which means external public relations, media, social media, communications management and similar costs, reasonably incurred by **you** with **our** prior consent, to avoid or mitigate harm to **your business** as a consequence of a **cyber event**.

l. **virus extraction costs** which means costs, reasonably incurred by **you** with **our** prior consent, to remove a virus from **your computer systems**.

11. **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**.

12. **defence costs** means the reasonable costs, charges, fees and expenses incurred, by **us** or by **you** with **our** prior written consent, to defend, investigate, appeal, or settle a **claim** or **multimedia claim**.

13. **direct financial loss** means

    a. unintended or unauthorised call charges or bandwidth charges in excess of **your** normal and usual amounts that **you** must pay caused by **telephone phreaking**; or

    b. unintended or unauthorised bandwidth charges and electricity costs in excess of **your** normal and usual amounts that **you** must pay caused by **cryptojacking**.

    The maximum **limits** for **direct financial loss** from **telephone phreaking** or **cryptojacking** are stated in **your schedule**.

14. **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; failure to pay salary or any other employment-related benefits; 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.

15. **essential service**, for the purposes of exclusion 10, means a service that is essential for the maintenance of vital functions of a **state** including without limitation: financial institutions and associated financial market infrastructure, health services or utility services.

16. **excess** means the amount of money that **you** are responsible for before **we** make a payment under the policy. The **excess**, including the **excess** for any optional cover, is set out in **your schedule**. If there is more than one **excess** stated in **your schedule** then

you will pay the higher **excess** if the incident or claim relates to that higher **excess**.

17. **identity theft** means the unauthorised use of the identity of an individual whose data or information has been accessed because of a **cyber event** that happens to **your computer systems**.

18. **impact on business costs** means:

    a. the amount that the **net profit you** earn during the **indemnity period** falls short, directly as a result of an **outage**, of the **net profit you** ordinarily earn, less any **net profit** that is subsequently recouped within a reasonable additional time period (which is not limited to the **indemnity period**) and less any consequent savings by **you**; and

    b. the net increased costs incurred during the **indemnity period** to avoid a reduction in **net profit** directly as a result of an **outage** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **net profit** 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 **impact on business costs** incurred during the **waiting period** after the **outage** occurs unless the first discovery of the **cyber event** occurred during a **preventative shutdown**.

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

    a. the functioning of that **state** due to the direct or indirect effect of the **cyber operation** on the availability, integrity or delivery of an **essential service** in that **state**; and/or

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

20. **indemnity period** means the period starting from discovery of the **cyber event** until **your computer systems** are restored to their usual function, however, in total length, not exceeding the number of days set out in **your schedule**.

21. **insured** means any person or entity entitled to cover under this **policy**.

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

23. **IT infrastructure** means all of the hardware, firmware, software, and networks, owned by or leased to, rented to, or licensed to **you** insofar as they are required to develop, test, deliver, monitor, control, or support IT services **you** use in **your business**. The term **IT infrastructure** includes all of the information technology but not the associated people, processes, and documentation. **IT infrastructure** does not include **operational technology**.

24. **limit** means the maximum amount set out in the **schedule** that **we** agree to pay for each insuring clause, extension, and optional cover, irrespective of the number of **claim**(s) **you** make under the **policy**. The **limit** or sublimit for any Optional Cover is also set out in **your schedule**.

25. **loss** means any sums payable pursuant to judgements (including orders for costs made against **you**), settlements, awards and determinations including damages, regulatory and civil fines, and penalties where insurable, in respect of a **claim** or **multimedia 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**.

26. **multimedia 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 and caused by or in connection with a **multimedia injury**.

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

    a. libel, slander, defamation;

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

    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;

    but only to the extent that the loss is solely occasioned by **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 by **you** of any patent.

28. **net profit** means the earnings of **your business** after deducting all operating expenses, interest and tax.

29. **operational technology** means hardware and software used to monitor or control physical processes and industrial operations in **your business** and includes Industrial Controls Systems (ICS), Supervisory Control And Data Acquisition (SCADA), and Internet of Things (IOT).

    Operational technology does not include **IT infrastructure**.

30. **outage** means the disruption of, disturbance to, or inability to access **your computer systems**.

31. **payment card industry liability** means the fines, penalties, and monetary assessments that **you** are legally liable to pay as a direct result of **your** noncompliance 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 date upon which **your senior management team** first becomes aware of **your** non-compliance with a Payment Card Industry Data Security Standard.

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

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

34. **policyholder** means the first named **insured** in **your schedule** under **Policyholder / Business** and which is authorised to enter into and deal with this **policy** on behalf of all **insureds**.

35. **preventative shutdown** means the reasonable, necessary, and intentional shutdown of **your IT infrastructure** in response to a reasonably suspected **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. a specific instruction from **your** financial institution, law enforcement or the Australian Signals Directorate or similar agency of the government; or
    c. a 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** or avoidance of otherwise larger claims under this **policy**.

36. **preventative shutdown allowance** means

    a. the amount that the **net profit you** earn during a **preventative shutdown** falls short, as a result of the **preventative shutdown**, of the **net profit you** ordinarily earn directly, less what is subsequently recouped within a reasonable additional time period (which is not limited to the **preventative shutdown** period) and less any consequent savings by **you**;
    b. the net increased costs incurred to avoid a reduction in **your net profit** 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 **net profit** in a. above. Net increased costs do not include **your** ongoing normal operating expenses, salaries, or overhead expenses; and
    c. reasonable and necessary costs, incurred by **you** with **our** prior agreement, 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** or the cost for **you** to implement critical security audit recommendations or other measures as required to mitigate the threat.

    Preventative shutdown allowance 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** after **you** initiate a preventative shutdown.

    The **excess** does not apply to the **preventative shutdown allowance**.

    We will pay a **preventative shutdown allowance** for up to a maximum of 72 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 – Business Interruption.

37. **records of your business** means all documents that evidence **your net profit**, including **your** bank records, GST records, tax records and usual business records including records that evidence **your** expenditure and outgoings.

38. **reputational harm impact** means:

    a. the amount that the **net profit you** earn during the **reputational harm period** falls short of the **net profit you** ordinarily earn solely and directly as a result of an **adverse media event**, less what is subsequently recouped within a reasonable additional time period not limited to the **reputational harm period**, and less any consequent savings, and

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

    Reputational harm impact does not include **cyber event response costs**.

39. **reputational harm period** means 60 days from the date of the first publication of an **adverse media event**.

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

41. **senior management team** means the **policyholder's** Managing Director, Chief Executive Officer, Chief Financial Officer, Chief Operations Officer, Chief Information Officer, Chief Information Security Officer, Chief Technology Officer, General Manager, General Counsel, Risk Manager, Insurance Manager, Privacy Officer, IT Manager, or equivalent role(s) at **your business**.

42. **state**, for the purposes of exclusion 10, means sovereign state.

43. **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**, **preventative shutdowns**, s**ystem failures** or **multimedia injury** that happen after the date of such formation or acquisition:

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

    b. the entity's revenue does not exceed 15% 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 claims**, or **multimedia claim**s prior to **you** acquiring it; and

    e. the entity's **computer systems** security controls and risk management are equal to or better than **yours**, or **you** will use best endeavours within a reasonable period of time either to bring its **computer systems** and risk management to an equivalent standard or to ensure its **computer systems** will be absorbed promptly into y**our computer systems**.

44. **system outage** means an **outage** caused solely by a **cyber event**.

45. **system failure** means an interruption to **your business** directly arising from an unintentional, unexpected, and unplanned **outage** of **your IT infrastructure** but does not include an **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**; or

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

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

47. **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.

    Utility provider does not include those services under **your** direct control.

48. **waiting period** means the number of hours specified in **your schedule**.

49. **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.

50. **we/our/us** means underwriters designated in the **schedule** as insurers of this **policy** and Emergence acting on behalf of underwriters as the issuer of this **policy**.

51. **you/your** means the **policyholder** referred to in **your schedule**, **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 H – Exclusions

Exclusions - all sections of the policy

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

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

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 caused to individuals other than **employees**, 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 **your** senior management team or discovered by **your** senior management team before the **policy** period.

4. arising from or based upon any intentional, criminal, or fraudulent acts by **you**. For the purposes of 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. arising from, attributable to, or as a consequence of ionising, radiation, or contamination by radioactivity from any nuclear fuel, waste or other hazardous properties of any nuclear assembly or component.

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

9. directly or indirectly involving the infringement of any copyright, service mark, trademark, or other intellectual property.

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

    a. **war** and/or
    b. a **cyber operation** that is carried out as part of **war**, or the immediate preparation for **war**, and/ or
    c. a **cyber operation** that causes a **state** to become an **impacted state**.

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

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

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

to another **state** or those acting at its direction or under its control.

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

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

    This exclusion does not apply to any such activities that are excluded under exclusion 10 (**war** or a **cyber operation**).

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

13. that was assumed by **you** under any contract unless **you** have a liability independent of the contract. This exclusion does not apply to a **payment card industry liability**.

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

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

16. arising from, attributable to, or as a consequence of theft by **you** or **your** employees other than theft of data.

17. 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.

18. arising from, attributable to, or as a consequence of any joint venture or consortium in which **you** have an interest. This exclusion does not apply to optional cover - joint venture and consortium cover.

19. in connection with any **claim** or **multimedia claim** made by one **insured** against any other **insured**, or against **you** by **your** parent company or by anyone with effective control over **you**. This exclusion does not apply to claims made against **you** by or on behalf of **your** employees.

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

21. in respect 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 infrastructure **you** sell, lease, license or otherwise provide to others for a fee.

22. in respect of any warranty for 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.

23. arising from, attributable to, or as a consequence of any financial **loss** due to **your** inability to trade, invest, divest, buy or sell any financial security or financial asset of any kind.

24. arising from any action of a public or governmental authority, including the expropriation, nationalisation, seizure, confiscation, or destruction of **your computer systems**. This exclusion does not apply to regulatory proceedings, investigations, or civil fines.

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

26. caused by defective equipment, ordinary wear or deterioration, faulty design or construction or insufficient capacity of **your computer systems**.

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

Exclusions - section C of the policy only

The following exclusions apply to Section C - Cyber & Privacy Liability only.

28. for an action brought against **your** directors or officers acting in that capacity or an action against **you** for providing services to others as an **IT contractor**.

29. 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.

Section I – 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**, **system failure**, **adverse media event**, if a **claim** or **multimedia 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 ring the Emergence reporting line on 1300 799 562 or notify Emergence in writing at claims@emergenceinsurance.com.au as soon as practicable and provide details and circumstances of the event, including any **claims**, **multimedia claims**, demands or notices received by **you** or proceedings against **you**.

2. **You** must report **telephone phreaking** or **cryptojacking** to, respectively, the Australian Cyber Security Centre, **your** telephone service provider (**telephone phreaking**) or utility provider (**cryptojacking**), as soon as practical after **you** first discover the **telephone phreaking** or **cryptojacking**.

3. **You** must do everything reasonably possible to preserve evidence to enable **us** to properly assess and investigate the claim.

4. If the claim is not covered under **your policy**, **we** will advise **you** to engage **your** own service resources.

5. **You** must fully cooperate with **our** technical management, **our** claims management, emergence's incident response team, and **our** investigation teams and with any providers **we** appoint.

6. **You** must do everything reasonably possible to assist in the reduction or mitigation of the **impact on business costs**, **loss**, **cyber event response costs**, **reputational harm impact**, or **direct financial loss**.

7. **You** must, at **your** own cost, provide all necessary information to **us** to enable **us** to assess the claim and any potential payment under this **policy**.

8. **We** will not reimburse **you** for any costs incurred by or payments made by **you** unless approved by **us** before they are incurred. **Our** consent will not be unreasonably withheld.

9. **Defence costs** must be approved by **us** before they can be incurred by **you**. **We** will not unreasonably withhold or delay **our** consent to **you** incurring reasonable and necessary **defence costs**.

10. **You** will pay the **excess** set out in **your schedule** before **we** make or incur any payment.

11. If cost is incurred in response to a **cyber event**, **preventative shutdown**, **system failure**, **claim**, or **multimedia claim** and some of that cost is not **impact on business costs**, **preventative shutdown allowance**, **loss**, **cyber event response costs**, **reputational harm impact**, 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** in our absolute discretion.

Section J – 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. 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**.

2. 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**, **preventative shutdow**n, **multimedia injury**, **adverse media events**, or **system failures** that happened prior to the date of such gaining of control or acquisition, unless **we** provide written agreement to extend coverage under the **policy** and **you** agree to the terms of any such extension of coverage.

3. This **policy** and any rights under it cannot be assigned without **our** written consent.

4. 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** under the **policy**. 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.

5. **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).

6. **We** will indemnify **you** for **claims** under Section C –Cyber & Privacy Liability, or **multimedia claims** under Section F – Multimedia Liability Cover, where the **claim** or **multimedia 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.

7. 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 any 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).

8. 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.

9. **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.

10. 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.

11. If **you** report a **cyber event**, **preventative shutdown**, **system failure**, **claim**, **multimedia claim**, **adverse media event** or **cryptojacking** to **us** and either, or all, of **impact on business costs**, **preventative shutdown allowance**, **loss**, **cyber event response costs**, **reputational harm impact**, 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.

12. All reported incidents and claims which arise out of one, or arise out of a series of related, **cyber events**, **preventative shutdowns**, **system failures**, or **multimedia injuries** involving **your computer system**s or **business** will be deemed to be one **cyber event**, **preventative shutdown**, **system failure**, or **multimedia injury** and only one **aggregate** will apply.

13. 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.

14. Where **you**:

    a. prior to the **policy period** first became aware of facts or circumstances that might give rise to a **claim** or **multimedia 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 **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** or **multimedia claim**.

15. If this **policy** is cancelled by either **us** or **you** for any reason other than non-payment of premium and no **claim** has been made under this **policy** and no other similar insurance has been arranged by **you**, 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** or **multimedia 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.

16. 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. 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.

17. 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 cosubscribing **insurer** who for any reason does not satisfy all or part of its obligations.

emergence

Bligh House, Suite 8.01
Level 8, 4-6 Bligh Street, Sydney NSW 2000
+61 1 300 799 562
emergenceinsurance.com.au