Cyber event protection

Important Information and Policy Wording

Cyber Insurance that moves with you into the 21st century

The team at Guild Insurance have partnered with Emergence to provide you with an insurance product designed to protect Australian business from the increasing threat of a cyber event.

Guild Insurance is acting as an agent of Emergence. Pursuant to an authority provided by Emergence for Guild to arrange and issue this policy on behalf of Emergence with the purpose of providing you with a progressive insurance product that moves with the ever changing digital landscape. This product will help safeguard your business, now and well into the future.

You must immediately ring the Emergence cyber event reporting line on **1300 799 562**.

After contacting **1300 799 562** you must also notify Emergence in writing at **emergence@cl-au.com** of the cyber event and any claim received by you for loss arising out of the cyber event.

Contents

Important Information

It is important that you read and understand the following:

About Emergence Insurance Pty Ltd

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

Contact details are:

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

Our agreement

Your contract with **us** consists of the **policy** wording together with the **schedule**, any endorsement(s) stated in **your schedule**, other documents **we** send to **you** and any supporting information **you** provide to **us**.

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**.
2. After contacting **1300 799 562 you** must also notify Emergence in writing at **emergence@cl-au.com** of the **cyber event** and any **claim** received by **you** for loss arising out of the **cyber event**.
3. **You** must report **cyber theft** or **telephone phreaking** to the police, and **telephone phreaking** to **your** telephone service provider, within 24 hours.
4. **We** will assess whether it is a **cyber event** or **claim** under the **policy**.
5. If it is a **cyber event** or **claim** under this **policy we** will implement a technical management response for **cyber event response costs**, a claims management response for **impact on business costs** and **loss**, and a criminal forensic response for **cyber theft**.
6. If it is not a **cyber event** or claim under this **policy we** will advise **you** to engage **your** own service resources.

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. Optional Covers may also be agreed, as set out in Section D.

Section A – Losses To Your Business responds to a **cyber event** in **your business** and covers reasonable costs to bring **your business** back to the condition it was immediately before the **cyber event**. These costs are called **impact on business costs**.

Section B – Loss To Others covers the **loss you** are legally liable to pay to others because of a **cyber event** in **your business** or because of **multimedia injury**. The **policy** also pays the costs of investigating and defending such **claims**.

Section C – Cyber Event Response Costs sets out the **cyber event response costs** that **we** pay in responding to a **cyber event**.

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** and **excess** for each Optional Cover will be stated in **your schedule**.

Section E – What Certain Words Mean explains the meaning of defined words used in the **policy**. These words may be used in one or more sections of the **policy.** The meaning of the words "**cyber event**" is also explained.

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

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

Section G – Claims Conditions explains what **you** must do if there is a **cyber event**.

Section H – General Conditions which **you** have to comply with under this **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 that **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** 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, 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 **policy**.

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.

Your 'cooling off' rights

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

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

Complaints

Step 1

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

By phone: +61 2 8280 3000

By email: **contractadmin@emergenceinsurance.com.au**

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

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

Step 2

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

By phone: +61 2 8298 0783

By email: **idraustralia@lloyds.com**

By fax: +61 2 8298 0788

In writing to: Level 9, 1 O'Connell St, Sydney NSW 2000

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

Step 3

If **we** are unable to resolve **your** complaint within 45 calendar days of the date **we** first received **your** complaint or if **you** remain dissatisfied, **you** may seek a free and independent review by the Financial Ombudsman Service Australia (FOS Australia) if **your** complaint falls within the FOS Terms of Reference. FOS Australia is an external dispute resolution scheme and their service is free to **you**. **We** agree to be bound by its decisions. **You** do not have to accept their decision and **you** have the right to seek legal advice at any time.

You can contact FOS Australia:

By phone: 1800 367 287 (or 1800 FOS AUS)

By Fax: +61 3 9613 6399

By email: **info@fos.org.au**

In writing to: Financial Ombudsman Service Australia GPO Box 3, Melbourne VIC 3001

By visiting: **fos.org.au**

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

General Insurance Code of Practice

We and Emergence proudly support the General Insurance Code of Practice. The purpose of the Code is to raise the standards of practice and service in the general insurance industry.

For further information on the Code, please visit **codeofpractice.com.au**

Privacy

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

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

We need to collect, use and disclose **your** personal information (which may include sensitive information) in order 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**.

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.

How this policy works

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. 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 **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 the Privacy Policy, please contact the Emergence Privacy Officer by:

Postal Address: PO Box A2016, Sydney South NSW 1235

Phone: +61 2 9307 6656

Fax: +61 2 9307 6699

Email: **privacyofficer@steadfastagencies.com.au**

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

Section A, B, C, D
Cover

Subject to payment of the **premium**, this **policy** will respond to a **cyber event** which is first discovered by **you** and notified to **us** during the **policy period**. **We** will pay up to the **limit** stated in the **schedule**. The aggregate **limit** is the most **we** will pay for all Sections, including any Optional Covers. The **limit** stated on **your schedule** is exclusive of GST.

Section A – Losses To Your Business

If a **cyber event** happens in **your business,** then **we** will pay **you** the **impact on business costs**.

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 reported to **us** during the **policy period** because of **multimedia injury** or because of a **cyber event** in **your business**.

Section C – Cyber Event Response Costs

If there is a **cyber event** in **your business,** then **we** will pay **your cyber event response costs.**

Section D – Optional Covers

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

The **limit** and **excess** for each Optional Cover, if applicable, will be stated in **your schedule** exclusive of GST. Optional Cover **limits** form part of and are included within the aggregate **limit**.

Optional Cover – Contingent Business Interruption Cover

We will pay **you impact on business costs** caused by an interruption to **your business** directly arising from an outage at **your** external suppliers' business, where, in **our** opinion, the outage has been caused by a **cyber event** at **your** external supplier's business.

Additional terms

For the purpose of this Optional Cover – Contingent Business Interruption Cover only, the words **cyber event** in the **policy** is extended to include a **cyber event** at **your** external supplier's business.

We will not pay any **impact on business costs** incurred under this Optional Cover – Contingent Business Interruption Cover during the waiting period of 7 days (168 hours) after the first interruption to **your business**.

For the purpose of this Optional Cover – Contingent Business Interruption Cover only, the words **indemnity period** in the **policy** is amended and means the period starting from the first interruption to **your business** until supply from **your** external supplier resumes, or until **you** have a substitute supply, plus reasonable additional time to allow **your business** and **revenue** to normalise however in total length not exceeding 35 days.

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

Optional Cover – Cyber Theft And Telephone Phreaking Cover

We will pay a **direct financial loss** to **you** or a **direct financial loss you** are legally liable to pay to others directly arising out of **cyber theft** or **telephone phreaking** that is first discovered by **you** and notified to **us** in the **policy period**.

Section F – Exclusion 19 of the **policy** is varied to the extent of this Optional Cover – Cyber Theft And Telephone Phreaking Cover.

For the purposes of this Optional Cover – Cyber Theft And Telephone Phreaking Cover only, the words listed below have been given a specific meaning and these specific meanings apply:

direct financial loss means

a. **your** funds or money, or the funds or money in **your** control belonging to others, that is lost due to **cyber theft** and remains unrecoverable, or

b. unintended or unauthorised call charges or bandwith charges in excess of normal and usual amounts that **you** must pay caused by **hacking** of **your** telephone systems.

You must report the **cyber theft** or **telephone phreaking** to the police, and **telephone phreaking** to **your** telephone service provider, within 24 hours of it first being discovered by **you**.

Optional Cover – Tangible Property Cover

We will pay the cost of the replacement or repair of any of **your IT infrastructure** that is physically damaged solely and directly because of a **cyber event** or the incurring of **cyber event response costs**.

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

Section A, B, C, D
Cover

Optional Cover – Joint Venture And Consortium Cover

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

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

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

Section F – Exclusion 21 of the policy is varied to the extent of this Optional Cover – Joint Venture And Consortium Cover.

Section E
What certain words mean

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

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

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**.

business activity statement means the Business Activity Statement (BAS) that is submitted by **your business** to the Australian Taxation Office for taxation purposes.

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

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

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

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

- **credit and identity monitoring costs** incurred in engaging monitoring services by a third party for persons affected by a **cyber event** for a period of up to 12 months.
- **cyber extortion costs** paid with **our** agreement and consent to respond to a **cyber event** where a third party is seeking to obtain financial gain from **you** through **cyber extortion**.
- **data restoration costs** incurred in restoring or replacing data or programs in **your IT infrastructure** that have been lost, damaged or destroyed and the cost to mitigate or prevent further damage and includes the cost of **you** purchasing replacement licences, if necessary, but does not include any costs relating to redesign, replication or reconstitution of proprietary information, facts, concepts or designs.
- **data securing costs** incurred in securing **your IT infrastructure** to avoid ongoing **impact on business costs**, **loss** and **cyber event response costs**.
- **external management costs** incurred in responding to a **cyber event** including crisis management and mitigation measures engaged in by **you** and agreed to by **us** when necessary to counter a credible impending threat to stage **a cyber event** against **your IT infrastructure**.
- **notification costs** incurred in notifying any person whose data or information has been wrongfully accessed or lost including the cost of preparing a statement to the Office of the Australian Information Commissioner or other authorities.
- **public relations costs** incurred in responding to a **cyber event** including external public relations, media, social media and communications management.

Section E
What certain words mean

- **pursuit costs** of up to a maximum of $50,000 paid with **our** agreement and consent to a third party (other than a law enforcement officer or **your** current or former employee or **IT contractor**), as reward for assistance leading to the arrest and conviction of the perpetrator of a **cyber event** covered under this **policy**.
- **virus extraction costs** incurred to remove a virus from **your IT infrastructure**.

cyber theft means the unauthorised electronic transfer of funds that results in the theft of funds or money that remain unrecoverable. The **cyber theft** must happen because of a **cyber event** that happens using **your IT infrastructure** without **your** knowledge.

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

employment wrongful act means any actual or alleged employment-related act, error, omission or conduct constituting actual, constructive or alleged: wrongful dismissal, discharge or termination of employment; wrongful failure to employ or promote; wrongful deprivation of career opportunity; misleading representation or advertising in respect of employment; wrongful disciplinary action; negligent employee evaluation; wrongful demotion; breach of employment contract; sexual or workplace harassment (including the creation of a workplace environment conducive to such harassment); wrongful discrimination; failure to grant tenure; invasion of privacy or defamation.

excess means the amount of money that **you** are responsible for before **we** make a payment under the **policy**. The **excess,** including the **excess** for any Optional Cover, is set out in **your schedule**.

impact on business costs means:

a. the amount by which the **revenue you** earn during the **indemnity period** falls short of the **revenue you** earned during relevant periods 12 months prior directly as a result of a **cyber event**, less any consequent savings. This is calculated by reference to the amounts shown on G1 (less the amount in G9) of **your business activity statement** for the prior relevant periods.

   If **you** have not been trading for a 12 month period **your** daily **revenue** during the **indemnity period** shall be calculated using the daily average **revenue** from G1 (less any amount in G9) in **your** most recent **business activity statement** less any savings in **your business** costs as a consequence of the **cyber event**, and

b. the net increased costs incurred to avoid a reduction in **revenue** as a consequence of a **cyber event** provided the amount of increased cost paid is less than **we** would have paid for a reduction in standard **revenue** in a. above.

We will not pay **impact on business costs** incurred during the waiting period of the first 12 hours after **you** discover a **cyber event** unless a different length of time has been specified on **your schedule**.

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

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

IT infrastructure means all of the hardware, firmware, software, networks, facilities, and the like, owned by or leased to, rented to or licensed to **you**, irrespective of where these are hosted, insofar as they are required to develop, test, deliver, monitor, control or support IT services used in **your business**. The term **IT Infrastructure** includes all of the information technology but not the associated people, processes and documentation.

limit means the amount set out in the **schedule** for each of Section A – Losses To Your Business, Section B – Loss To Others and Section C – Cyber Event Response Costs of **your policy** and applies to any one **cyber event**, irrespective of the number of claim(s). The **limit** for any Optional Cover is also set out in **your schedule**. One aggregate **limit** applies to **your policy** for the entire **policy period** and is set out in **your schedule**. The aggregate **limit** is the most **we** will pay, including **defence costs**, irrespective of the number of **cyber events**, **losses**, **claims** or insureds, for all Sections, including all Optional Covers.

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

multimedia injury means loss to others because of unintentional:

a. libel, slander, defamation;
b. infringement of trademark, service mark, slogan, copyright, domain name or metatags;
c. improper deep linking, framing, or web harvesting;
d. non-conformance with any legal requirement relating to web access such as the Disability Discrimination Act of 1992; or
e. inadvertent disclosure of personal information;

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

policy means this document, the **schedule** and any endorsement(s) stated in **your schedule**. The proposal form and other supporting information **you** provide to **us** are also incorporated into this **policy**.

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**.

revenue means the money paid or payable to **you** for goods sold, work done and services rendered in the course of **your business** and is calculated on the basis specified in the definition of **impact on business costs**.

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

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

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

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

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

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

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

telephone phreaking means a **hacking** of **your** telephone systems that results in **your** telephone systems incurring unintended or unauthorised call charges or bandwith charges.

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

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

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

you/your means the **policyholder** referred to in **your schedule**. It includes **your subsidiaries** together with any current, future or former employee, 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. For purposes of Optional Cover – Joint Venture And Consortium, it also includes any joint venture or consortium declared to **us** and designated in **your schedule**.

Section F
Exclusions

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

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

1. arising from or for physical damage to or the repair or replacement of tangible property or equipment.
2. arising from or as a consequence of death or bodily injury, however, this exclusion shall not apply to mental illness as a result of a **cyber event** and for which **you** are legally liable.
3. arising from any **cyber event**, loss, fact or circumstance known to **you** or discovered by **you** before the **policy period**.
4. arising from or based upon any intentional, criminal or fraudulent acts by **you**. For the purpose of applying this exclusion the acts, knowledge or conduct of any person covered under this **policy** will not be imputed to any other person covered under this **policy**.
5. arising from or as a consequence of **your** bankruptcy, liquidation or insolvency or the bankruptcy, liquidation or insolvency of any of **your IT contractors** or external suppliers.
6. arising from, or resulting in or causing an **employment wrongful act**.
7. for an action brought against **your** directors or officers acting in that capacity or an action against **you** for an error or omission while acting in a professional or fiduciary capacity or an action against **you** for providing services to others as an **IT contractor**.
8. in connection with any products, hardware, software, software as a service, platform as a service, infrastructure as a service, or related services or IT infrastructure **you** sell, lease, license or otherwise provide to others for a fee.
9. arising from, attributable to, or as a consequence of ionising, radiation or contamination by radioactivity from any nuclear fuel, waste or other hazardous properties of any nuclear assembly or component.
10. arising from, attributable to, or as a consequence of pollution.
11. directly or indirectly involving the infringement of any copyright, service mark, trade mark or other intellectual property, however this exclusion shall not apply to **multimedia injury** expressly covered under Section B.
12. arising from any physical act of war, invasion or warlike operation, civil war, riot, civil commotion, rebellion, revolution, insurrection or civil uprising.
13. caused by or arising out of any **act of terrorism**, however, this exclusion does not apply to:
    a. the following **cyber events**: **crimeware, cyber espionage, cyber extortion, denial of service**, distributed **denial of service hacking, payment card skimming**, **point of sale intrusion**, **web app attacks**;
    b. Optional Cover – **Cyber Theft** And **Telephone Phreaking** Cover.
14. arising from, attributable to, or in consequence of any electromagnetic field, electromagnetic radiation or electromagnetism.
15. that was assumed by **you** under any contract unless **you** have a liability independent of the contract.
16. that is related to damages characterised or described as aggravated, punitive or exemplary damages.
17. caused by defective equipment, ordinary wear or deterioration, faulty design or construction or insufficient capacity of **your IT infrastructure**.
18. arising out of or caused by outage of a **utility provider**.
19. caused by **cyber theft** or **telephone phreaking**. This exclusion does not apply to **cyber event response costs** incurred solely and directly due to **cyber theft** or **telephone phreaking**.
20. to the extent that the provision of such cover, payment of such claim or provision of such benefit would expose **us** or any (re)insurer to any sanction, prohibition or restriction under United Nations resolutions or the trade or economic sanctions, laws or regulations of the European Union, United Kingdom or United States of America.
21. arising from, attributable to, or as a consequence of any joint venture or consortium in which **you** have an interest.
22. in connection with any **claim** made by one insured against any other insured under this **policy**, or against **you** by **your** parent company or by anyone with effective control over **you**.
23. arising from, attributable to, based upon or in connection with any **claim, loss,** judgement or award made in the United States of America or which applied the laws of the United States of America.
24. directly or indirectly involving any actual or alleged infringement of any patent.

Section G
Claims Conditions

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

1. **You** must immediately ring the Emergence **cyber event** reporting line on **1300 799 562**.
2. After contacting **1300 799 562 you** must also notify Emergence in writing at **emergence@cl-au.com** of the **cyber event** and any **claim** received by **you** for loss arising out of the **cyber event**.
3. **You** must report **cyber theft** or **telephone phreaking** to the police, and **telephone phreaking** to your telephone service provider, within 24 hours.
4. **We** will assess whether it is a **cyber event** or **claim** under the **policy**.
5. If it is a **cyber event** or **claim** under this **policy we** will implement a technical management response for **cyber event response costs,** a claims management response for **impact on business costs** and **loss**, and a criminal forensic response for **cyber theft**.
6. If it is not a **cyber event** or **claim** under this **policy we** will advise **you** to engage **your** own service resources.
7. **You** are required to fully cooperate with **our** technical management, claims management and criminal forensic response teams and with any providers **we** appoint.
8. **You** must do everything reasonably possible to assist in the reduction or mitigation of the **impact on business costs, loss, cyber event response costs** or **direct financial loss**.
9. **You** must, at **your** own cost, provide all necessary information to **us** to enable **us** to assess **impact on business costs**, a **loss**, **cyber event response costs** or **direct financial loss**.
10. If **you** do not accept **our** assessment of **impact on business costs** and **we** agree to **you** incurring **preparation costs**, **we** will pay up to a maximum amount of $10,000 for **preparation costs**.
11. **We** will not reimburse **you** for any costs incurred by or payments made by **you** unless approved by **us**.
12. **Defence costs** must be approved by **us** before they can be incurred by **you**.
13. If **you** report a **cyber event** or **claim** to **us** and either, or all, of **impact on business costs**, a **loss**, **cyber event response costs** or **direct financial loss** are incurred then **we** will apply the aggregate **limit** and **excess** set out in **your schedule** as if one **cyber event** happened.
14. **You** will pay the **excess** set out in **your schedule** before **we** pay or incur a payment.
15. If cost is incurred in response to a **cyber event** or **claim** and some of that cost is **not impact on business costs, loss, cyber event response costs** or **direct financial loss** it is **your** responsibility to pay some or all of the cost. **We** will determine a fair and reasonable allocation of cost between what is covered and what is not covered under the **policy**.

Section H
General Conditions

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

1. **You** must immediately notify **us** 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; or
   b. **you** become aware of a pending appointment of a receiver or the commencement of bankruptcy or winding up proceedings to **your business**; or
   c. if **you** form or acquire an entity that does not meet the criteria for automatic inclusion under this **policy** as set forth in the definition of **subsidiary**.
3. **You** must maintain I.T. security practices and procedures to a standard equal to or better than as existed at the time this **policy** commenced. A failure to adhere to such practices and procedures by an employee or **your IT contractor** shall not constitute a breach of this condition.
4. If during the **policy period** any other entity gains control of management or acquires more than 50 percent of the **policyholder** or any **subsidiary**, this **policy** shall be restricted in respect of the **policyholder** or that **subsidiary** so as to apply only to **cyber events** that were first discovered and **claims** that were first made 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 on account of a **cyber event response cost**.

   It is **your** responsibility to inform **us** whether or not **you** are entitled to an Input Tax Credit for any amounts claimed under this **policy**.

   All **policy limits** stated on **your schedule** are exclusive of GST.
7. **You** may cancel the **policy** in accordance with **your** 'cooling off rights' within the first 14 days from commencement.

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

   We can only cancel the **policy** in accordance with the provisions of the **Insurance Contracts Act 1984 (Cth).**
8. This **policy** including its construction, application and validity, is governed by the laws of the Commonwealth of Australia and/or the State or the Territory of Australia where the **policy** was issued. Any dispute relating to the interpretation of this **policy** will be submitted to the exclusive jurisdiction of the Courts of the State or Territory where the **policy** was issued.
9. **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.
10. 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).**
11. If at the time any claim arises under this **policy** there is any other insurance in force covering the same loss, in part or in full, **you** must promptly notify **us** of full details of such other insurance, including the identity of the insurer(s) and the policy number(s), and such further information as **we** may reasonably require. Subject to the **Insurance Contracts Act 1984** (Cth), **we** reserve the right to seek a contribution from the other insurer(s).
12. **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.
13. 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.

14. 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**.

15. If this **policy** is terminated by either **us** or **you** for any reason other than non payment of premium and provided no **cyber event** has occurred, no claim has been made and/or 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 **cyber events** first discovered by **you** and **claims** first made against **you** prior to termination and notified to **us** during the extended reporting period.

16. The underwriters 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 underwriters 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 underwriters may be served upon:

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

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

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

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

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 co-subscribing insurer who for any reason does not satisfy all or part of its obligations.

Guild INSURANCE

For more information call
1800 810 213

or visit
guildinsurance.com.au

To make a claim call
1300 799 562

GLD3690 Cyber Event Protection PDS 06/2018.