

Cyber Enterprise Risk Management *Version 2.2* Policy

Policy Wording and Schedule

CHUBB®

Contents

| | |
|--|----|
| Duty of Disclosure..... | 3 |
| Policy Schedule | 4 |
| Cyber Enterprise Risk Management Version 2.2 Endorsement(s)..... | 7 |
| 1. Insuring Agreements | 8 |
| 2. Insuring Agreement Extensions | 9 |
| 3. General Definitions | 10 |
| 4A. Exclusions Applicable to Definitions (Section 3)..... | 23 |
| 4. General Exclusions..... | 26 |
| 5. General Conditions | 26 |
| Privacy Statement | 39 |
| General Insurance Code of Practice..... | 41 |
| Complaints and Dispute Resolution Process | 41 |
| About Chubb in Australia | 43 |
| Contact Us..... | 43 |

Cyber Enterprise Risk Management *Version 2.2* Policy

Policy Wording and Schedule

Duty of Disclosure

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, extend, vary or reinstate an insurance contract.

What You do not need to tell us

You do not need to tell us anything that:

- reduces the risk We insure You for; or
- is common knowledge; or
- We know or should know as an insurer; or
- We waive Your duty to tell us about.

If You do not tell us something

If You do not tell us anything You are required to, We may cancel Your contract or reduce the amount We will pay You if You make a claim, or both.

If Your failure to tell Us is fraudulent, We may refuse to pay a claim and treat the contract as if it never existed.

Policy Schedule

| | | | | |
|-----------------------|--|--|------------------------|-----------------------|
| Policy Number: | | | | |
| Item 1: | Named Insured | | | |
| | Principal Address | | | |
| Item 2: | Policy Period | From: | L.S.T | |
| | | To: | L.S.T | |
| | | <i>Both days inclusive</i> | | |
| Item 3 | Policy Aggregate: | | | |
| | First Party Insuring Agreements | | Aggregate Limit | Excess |
| | Incident Response | in respect of a Covered Computer System | | |
| | | in respect of a Shared Computer System | | |
| | Business Interruption | in respect of a Covered Computer System | | Waiting Period: hours |
| | | in respect of a Shared Computer System | | Waiting Period: hours |
| | Data and System Recovery | in respect of a Covered Computer System | | |
| | | in respect of a Shared Computer System | | |
| | Cyber Extortion | in respect of a Covered Computer System | | |
| | | in respect of a Shared Computer System | | |
| | Third Party Insuring Agreements | | Aggregate Limit | Excess |
| | Privacy and Network Security Liability | | | |
| | Media Liability | | | |
| | Insuring Agreement Extensions | | Aggregate Limit | Excess |
| | Emergency Incident Response | in respect of a Covered Computer System | | |
| | | in respect of a Shared Computer System | | |
| | Betterment Costs | | | |
| Cyber Crime | in respect of a Covered Computer System | | | |

| | | | | | |
|---------------|---|---|------------------------------------|------------------------------------|---------------|
| | | in respect of a Shared Computer System | | | |
| | Reward Expenses | | | | |
| | Telecommunications Fraud | in respect of a Covered Telecom System | | | |
| | | in respect of a Shared Telecom System | | | |
| | Sub-Limits | | Sub-Limited Aggregate Limit | Excess | |
| | Consumer Redress Fund | | | | |
| | Payment Card Loss | | | | |
| | Regulatory Fines | | | | |
| | Additional Sub-Limits | Coinsurance Percentage | | Sub-Limited Aggregate Limit | Excess |
| | Ransomware | | | | |
| | Neglected Software Exploit | 0 - 45 days | 0 % | | |
| | | 46 - 90 days | 5% | | |
| | | 91 - 180 days | 10% | | |
| | | 181 - 365 days | 25% | | |
| | | Longer than 365 days | 50% | | |
| | Sub-Limits for Widespread Events | Coinsurance Percentage | | Sub-Limited Aggregate Limit | Excess |
| | Widespread Severe Known Vulnerability Exploit | | | | |
| | Widespread Software Supply Chain Exploit | | | | |
| | Widespread Severe Zero Day Exploit | | | | |
| | All Other Widespread Events | | | | |
| Item 4 | Retroactive Date: | | | | |
| Item 5 | Policy Form: | Cyber Enterprise Risk Management Version 2.2 Policy | | | |

| | | |
|---------------|-------------------------------------|-----------|
| Item 6 | Premium (excluding taxes) | As Agreed |
| Item 7 | Period of Indemnity: | |

Signed for and on behalf of Chubb Insurance Australia Limited

Date

Authorised Employee

Optional Cyber Risk Improvement Services

Services available to policyholders

Chubb is committed to helping Our clients' improve their cyber risk management practices. We have partnered with a number of dedicated cyber security vendors to offer risk improvement services to Our Chubb Cyber ERM policyholders. The services, designed to address common cyber threats and exposures, are detailed below. Visit www.chubb.com/cyber-services for more information.

| | |
|---|---|
| Cyber Alert App <i>provided by Chubb</i> | <p>The <u>Cyber Alert App</u> offers 24/7 incident reporting from a mobile device or computer and allows clients to pre-register contact details and policy information for efficient incident response management.</p> <hr/> <p>Additional Cost: <i>No cost</i> – available for download on iPhone and Android devices.</p> |
| Password Management Application <i>provided by Dashlane</i> | <p>The <u>Password Management Application</u> protects and manages passwords for users, providing a solution that remembers and automatically fills in passwords, logins, personal info, and payment details, encouraging responsible password usage. Dashlane also assists with Dark Web Monitoring and threat alerts for users.</p> <hr/> <p>Additional Cost: <i>No cost</i> – 500 complimentary individual licenses are available to all Chubb Cyber ERM policyholders.</p> |
| Phishing Awareness Training <i>provided by Cofense</i> | <p><u>Phishing Awareness Training</u> includes two simulated real-life phishing scenarios over the course of four months for up to 500 employees. At the end of the programme, results will be compiled into a useful report with extensive analytics, including an executive summary of the campaign, its findings, susceptibility rates and more. Risk improvement recommendations will be provided to help You once the programme ends.</p> <hr/> <p>Additional cost: AUD 3,900 <i>separate from Your insurance premium</i></p> |

For more information on these services and registration instructions, please visit www.chubb.com/cyber-services

Cyber Enterprise Risk Management Version 2.2 Endorsement(s)

1. Insuring Agreements

If "Not Covered" is shown in Item 3 of the **Schedule** in relation to any Insuring Agreement, such Insuring Agreement and any reference to it is deemed deleted and such coverage is not afforded.

First Party Insuring Agreements

We will pay on **Your** behalf for:

1.1 *Incident Response*

Incident Response Expenses by reason of a **Cyber Incident** or a **Business Interruption Incident** discovered by any **Control Group** member during the **Policy Period** and reported to **Us** pursuant to General Condition 5.10 Notification.

We will reimburse **You** for:

1.2 *Business Interruption*

Business Interruption Loss during the **Period of Indemnity**, arising from a **Business Interruption Incident** that exceeds the **Waiting Period** in duration, and is discovered by any **Control Group** member during the **Policy Period**;

1.3 *Data and System Recovery*

Data and System Recovery Costs during the **Period of Indemnity**, arising from a **Business Interruption Incident** discovered by any **Control Group** member during the **Policy Period**; and

1.4 *Cyber Extortion*

Cyber Extortion Damages and **Cyber Extortion Expenses** by reason of a **Cyber Extortion Event** discovered by any **Control Group** member during the **Policy Period**;

and reported to **Us** pursuant to General Condition 5.10 Notification.

Third Party Insuring Agreements

We will reimburse **You** for:

1.5 *Privacy and Network Security Liability*

Damages and **Privacy and Network Security Claims Expenses** by reason of a **Privacy and Network Security Claim** first made during the **Policy Period** resulting from any **Privacy and Network Security Wrongful Act** taking place after the **Retroactive Date** and prior to the end of the **Policy Period**; and

1.6 *Media Liability*

Damages and Media Claims Expenses by reason of a **Media Claim** first made during the **Policy Period** resulting from any **Media Wrongful Act** taking place after the **Retroactive Date** and prior to the end of the **Policy Period**;

and reported to **Us** pursuant to General Condition 5.10 Notification.

2. Insuring Agreement Extensions

If "Not Covered" is shown in Item 3 of the **Schedule** in relation to any Insuring Agreement Extension, such Insuring Agreement Extension and any reference to it is deemed deleted and such coverage is not afforded.

We will pay on **Your** behalf for:

2.1 *Emergency Incident Response*

Emergency Incident Response Expenses incurred within the first 48 hours immediately following the discovery of a **Cyber Incident** or **Business Interruption Incident** by any **Control Group** member during the **Policy Period** and reported to **Us** pursuant to General Condition 5.10 Notification, which requires immediate attention in order to mitigate the damage from, effects of and costs related to such **Cyber Incident** or **Business Interruption Incident**.

We will reimburse **You** for:

2.2 *Betterment Costs*

Betterment Costs arising from a **Business Interruption Incident** as covered under Insuring Agreement 1.3;

2.3 *Cyber Crime*

Direct Financial Loss solely as a result of **Theft** of the **Insured Organisation's Money or Securities** due to **Malicious Use or Access** of:

- (i) a **Covered Computer System**; or
- (ii) a **Shared Computer System**,

by a **Third Party** and discovered during the **Policy Period**;

2.4 *Reward Expenses*

Reward Expenses solely to the extent used in direct connection with a **Cyber Extortion Event** as covered under Insuring Agreement 1.4;

2.5 *Telecommunications Fraud*

Telecommunications Expenses due to a **Telecom Malicious Act** or **Malicious Use or Access** of:

- (i) a **Covered Telecom System**; or
- (ii) a **Shared Telecom System**,

by a **Third Party**, discovered by any **Control Group** member during the **Policy Period**;

and reported to **Us** pursuant to General Condition 5.10 Notification.

3. General Definitions

When used in this **Policy**:

- 3.1 **Accepted Program** means a program that has been fully developed, successfully tested and proved successful in an equivalent operational environment prior to release.
- 3.2 **Aggregate Limit** means the amount stated as such in the **Schedule** which, subject to the **Policy Aggregate**, is the maximum aggregate amount of any **Loss** and other covered amounts payable by **Us** under each Insuring Agreement and each Insuring Agreement Extension in respect of the **Policy Period**, irrespective of the number of **Claims**, the number of Sub-Limits, number of claimants, number of **Insureds** making a claim, number of Insuring Agreements and/or Insuring Agreement Extensions claimed under and/or anything whatsoever, including any combination of those things.
- 3.3 **Betterment Costs**, applicable to Insuring Agreement Extension 2.2 only, means costs to replace or restore software or applications in a **Covered Computer System** with newer, upgraded and/or improved versions of such software or applications.

Betterment Costs as provided for under Insuring Agreement 2.2 shall be part of and not in addition to the applicable **Aggregate Limit** shown in the **Schedule** for Data and System Recovery and shall reduce such applicable **Aggregate Limit**.

- 3.4 **Bodily Injury** means injury to the body, sickness, or disease, and death. **Bodily Injury** also means mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock, regardless of how it is caused or manifests, except that **Bodily Injury** does not include any mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock that arises out of a **Privacy and Network Security Wrongful Act** or **Media Wrongful Act** as expressly covered under Insuring Agreements 1.5 or 1.6.
- 3.5 **Business Interruption Incident** means inability to access, disruption of, or disturbance to:
- (i) a **Covered Computer System** or the taking of, corruption of or destruction of **Data** stored on a **Covered Computer System**; or
 - (ii) a **Shared Computer System** or the taking of, corruption of or destruction of **Data** stored on a **Shared Computer System**;

caused solely and directly by:

- A. a Computer Malicious Act;
 - B. **Unauthorised Use or Access**;
 - C. **Human Error**;
 - D. a failure of **Network Security**;
 - E. **Programming Error**;
 - F. the reasonable and necessary shutdown of all or parts of a **Covered Computer System** or a **Shared Computer System** in an attempt to mitigate the effects of any of items A.-E. above; or
 - G. solely in respect of paragraph (i) of this Definition, above, a power failure, surge or diminution of an electrical system controlled by **You**, which is a result of A, B, or D above
- 3.6 **Business Interruption Loss** means **Your Net Profit** before income taxes that would have been earned had the **Business Interruption Incident** not occurred, less **Your Net Profit** actually earned before income taxes.

Business Interruption Loss does not include amounts covered above that are accrued during the **Waiting Period**.

The **Excess** applicable to **Business Interruption Loss** shall be calculated pursuant to General Condition 5.5, D.

- 3.7 **Claim** means a **Privacy and Network Security Claim**, a **Media Claim**, and/or a **Wrongful Act**.
- 3.8 **Coinsurance** means the applicable percentage value listed at Item 3 of the **Schedule** that, with regards to coverage under the applicable Insuring Agreement or Insuring Agreement Extension, represents the amount of any **Loss** for each and every **Single Claim** which, after satisfaction of any applicable **Excess**, **You** shall bear at **Your** own risk and shall be uninsured by **Us**. **Coinsurance** shall be applied pursuant to General Condition 5.4 (Policy Limits).
- 3.9 **Computer Malicious Act** means any malicious act committed against a **Covered Computer System** or a **Shared Computer System**, or malicious access to or hacking of a **Covered Computer System** or a **Shared Computer System**, for the purpose of creating, deleting, taking, collecting, altering or destroying **Data** or services, without involving any physical damage to a **Covered Computer System** or a **Shared Computer System**, telecommunications equipment or infrastructure. **Computer Malicious Act** includes a distributed denial of service attack or the introduction of malicious code, ransomware, cryptoware, virus, trojans, worms and logic or time bombs or any malware, programs, files or instructions of a malicious nature which may disrupt, harm, impede access to, or in any other way corrupt the operation of a **Covered Computer System**, a **Shared Computer System**, **Data**, or software within.
- 3.10 **Computer System** means computer hardware, software, firmware, and the data stored on such hardware, software or firmware, as well as associated mobile devices, input and output devices, data storage devices, networking equipment and storage area network or other electronic data backup facilities, including SCADA and ICS systems.
- 3.11 **Consumer Redress Fund** means a sum of money that **You** are legally obligated to deposit in a fund as equitable relief for the payment of consumer **Privacy and Network Security Claims** or **Media Claims** due to an adverse judgment or settlement of a **Regulatory Proceeding**. **Consumer Redress Fund** shall not include any sums paid which constitute taxes, fines, penalties, injunctions or sanctions.
- 3.12 **Control Group** means the Chief Finance Officer, Chief Executive Officer, General Counsel, Risk Manager, Chief Information Officer, Chief Information Security Officer, Chief Technology Officer, Data Protection Officer, **Insurance Representative**, or the organisational equivalent of any of those positions of the **Named Insured**.
- 3.13 **Covered Computer System** means a **Computer System**:
- A. leased, owned, or operated by **You**; or
 - B. operated solely for **Your** benefit by a third party service provider under written agreement or contract with **You**.
- 3.14 **Covered Telecom System**, applicable to Insuring Agreement Extension 2.5 only, means:
- A. **Your** fixed line telecom system; or
 - B. a fixed line telecom system operated solely for **Your** benefit by a third party service provider under a written agreement or contract with **You**.
- 3.15 **Cyber Extortion Damages** means **Money**, including cryptocurrency(ies), paid by **You** where legally allowed and insurable, to terminate or end a **Cyber Extortion Event**. The valuation of **Cyber Extortion Damages** shall be calculated as described in General Condition 5.12.

- 3.16 **Cyber Extortion Event** means any credible threat or connected series of credible threats made against **You** expressing intent to perform or cause, or the actual performance of or causing of, the following:
- A. the release, divulgence, dissemination, destruction or use of confidential, sensitive or proprietary information, or personally identifiable information, stored on a **Covered Computer System** or a **Shared Computer System**;
 - B. a failure of **Network Security** on a **Covered Computer System** or a **Shared Computer System**;
 - C. the introduction or infliction of a **Computer Malicious Act** on a **Covered Computer System** or a **Shared Computer System**;
 - D. the alteration, corruption, destruction, misappropriation, manipulation of, or damage to, **Data**, instructions or any electronic information transmitted or stored on a **Covered Computer System** or a **Shared Computer System**; or
 - E. the restriction or inhibition of access to a **Covered Computer System** or a **Shared Computer System**;

for the purpose of demanding **Money** or cryptocurrency(ies) from **You**, or that **You** otherwise meet a demand, in exchange for the mitigation or removal of such threat or connected series of threats, or the reversal or termination of the actual performance of such threats or series of connected threat

Cyber Extortion Event shall not include any threats or connected series of threats made against **You** expressing intent to perform or cause any of the above if made, approved or directed by a member of the Control Group.

- 3.17 **Cyber Extortion Expenses** means such reasonable expenses to hire a third party consultant for the sole purpose of handling the negotiation and payment of **Cyber Extortion Damages** to terminate or end a **Cyber Extortion Event**.

- 3.18 **Cyber Incident** means any actual:

- A. **Computer Malicious Act, Human Error, Programming Error**, failure of **Network Security**, or **Unauthorised Use or Access** or any other threat or action against a **Covered Computer System**, including those threats or actions done in the commission of a **Cyber Extortion Event**;
- B. **Privacy and Network Security Wrongful Act**;
- C. power failure, surge or diminution of an electrical system controlled by **You** which is a result of a **Computer Malicious Act**, an **Unauthorised Use or Access** or a failure of **Network Security**; or
- D. **Telecom Malicious Act**;

that leads to the incurring of **Incident Response Expenses** to address such circumstances.

- 3.19 **Damages** means compensatory damages, any award of prejudgment or post judgment interest and settlements which **You** become legally obligated to pay as a result of a **Wrongful Act** to which this **Policy** applies.

Damages include punitive damages and exemplary damages, only to the extent such damages are insurable under the laws of the applicable jurisdiction that most favours coverage for such damages.

With respect to Insuring Agreement 1.5, **Damages** shall also include a **Consumer Redress Fund**, **Payment Card Loss**, and **Regulatory Fines**.

Any and all **Damages** are subject to the applicable **Aggregate Limit** or Sub-Limited **Aggregate Limit** listed on the **Schedule**.

Damages shall not include:

- a) any amount for which **You** are not legally obligated to pay;
- b) matters uninsurable under the laws pursuant to which this **Policy** is construed;
- c) the cost to comply with any injunctive or other non-monetary or declaratory relief, including specific performance, or any agreement to provide such relief;
- d) **Your** loss of fees or profits, return of fees, commissions;
- e) royalties, or re-performance of services by **You** or under **Your** supervision;
- f) disgorgement of any profit, remuneration or financial advantage to which **You** are not legally entitled;
- g) any amounts other than those which compensate solely for a loss caused by a **Wrongful Act**, unless specifically provided for in this **Policy**.

With respect to Insuring Agreement 1.5, **Damages** shall not include any amounts owed or paid by or to an **Insured**, which arise solely under a contract or agreement to the extent they exceed the amount for which you would otherwise be liable for in absence of the contract or agreement, including any royalties, restitution, reduction, disgorgement or return of any payment, charges, or fees; or costs to correct or re-perform services related to **Products**, including for the recall, loss of use, or removal of **Products**.

3.20 **Data** means any software or other information in electronic form which is stored on a **Covered Computer System** or a **Shared Computer System**. **Data** shall include the capacity of a **Covered Computer System** or a **Shared Computer System** to store information, process information, and transmit information over the Internet. **Data** shall not include or be considered tangible property.

3.21 **Data and System Recovery Costs** means any reasonable costs:

- A. to recover or reconstruct any **Data** that has been damaged, compromised or lost. These costs to recover or reconstruct **Data** are only available up and until a reasoned determination has been made by the third party forensics firm retained to recover the lost **Data**, that the **Data** cannot be recovered or reconstructed;
- B. to repair or restore software or applications in a **Covered Computer System** or a **Shared Computer System** but only if necessary to restore a **Covered Computer System** or a **Shared Computer System** to the same or equivalent condition or functionality as existed before the **Business Interruption Incident**;
- C. to identify and remediate the cause of the **Business Interruption Incident**; and
- D. with **Our** prior consent, which will not be unreasonably withheld or delayed:
 - (i) to update, upgrade, replace, or improve a **Covered Computer System** or a **Shared Computer System**, but only where the costs to update, upgrade, replace or improve the damaged or compromised software or applications on a **Covered Computer System** or a **Shared Computer System** to a newer or improved standard, condition, functionality, or version are reasonably expected by **You** to be less than or equal to the cost(s) to repair, fix or restore the same; or
 - (ii) to update, upgrade, replace, or improve a **Covered Computer System**, but only where **Betterment Costs** are applicable; and
 - (iii) any other reasonable costs to get **Your** business back to full operating condition, but only to the extent that the **Business Interruption Incident** solely created or caused the issue or problem that prevented **Your** business from being fully operational.

Data and System Recovery Costs include, but are not limited to:

- a) the use of external equipment whether by hiring a third party or leasing the equipment;

- b) the implementation of an alternate work method in accordance with a business continuity plan;
- c) costs to subcontract with an external service provider; and
- d) increased costs of labour.

Data and System Recovery Costs do not include:

- a) costs or expenses incurred to identify or remediate software vulnerabilities;
- b) costs to replace any hardware or physical property;
- c) costs incurred to research and develop **Data**, including **Trade Secrets**;
- d) the economic or market value of **Data**, including **Trade Secrets**;
- e) any other loss or damage which does not result directly from the **Business Interruption Incident**
- f) Incident Response Expenses; or
- g) costs to update, upgrade, replace, maintain, or improve any **Data** or **Computer System** beyond what is provided in General Definition 3.21, D, (i) and (ii).

3.22 **Direct Financial Loss**, applicable to Insuring Agreement Extension 2.3 only, means the replacement value of the **Money** or the market value of **Securities** at the time the **Theft** was discovered during the **Policy Period**. The valuation of **Direct Financial Loss** shall be calculated as described in General Condition 5.12

3.23 **Emergency Incident Response Expenses**, applicable to Insuring Agreement Extension 2.1 only, means those reasonable expenses:

- A. to retain the services of a cyber incident response manager for the purpose of coordinating response to **Your** confirmed **Cyber Incident** or **Business Interruption Incident**; and
- B. to retain a third party computer forensics firm to determine the cause and scope of **Your** confirmed **Cyber Incident** or **Business Interruption Incident** and to initiate the process to stop, reverse or remediate the effects of such **Cyber Incident** or **Business Interruption Incident**.

Emergency Incident Response Expenses shall be a part of and not in addition to the applicable **Aggregate Limit** shown in the **Schedule** for Incident Response as provided for under Insuring Agreement 1.1, and shall reduce and may completely exhaust such applicable **Aggregate Limit**.

3.24 **Excess** means the first part of a **Loss** and any other covered amount payable which shall apply to each and every **Claim**. The **Excess** that shall be borne by **You** is the amount listed on the **Schedule** with regard to coverage under the applicable Insuring Agreement or Insuring Agreement Extension. The **Excess** shall be applied pursuant to General Condition 5.5.

3.25 **Expenses** mean **Privacy and Network Security Claims Expenses, Media Claims Expenses, Cyber Extortion Expenses, Business Interruption Loss, Cyber Extortion Damages, Data and System Recovery Costs, and Incident Response Expenses. Expenses** shall also mean **Betterment Costs, Emergency Incident Response Expenses, Direct Financial Loss, Reward Expenses** and/or **Telecommunications Expenses**.

3.26 **Extended Reporting Period** means the period(s) for the extension of coverage, if applicable, described in General Condition 5.8 and 5.16.

3.27 **Human Error** means an operating error or failure to act, including the choice of the program used, an error in setting parameters or any inappropriate single intervention of:

- (i) the **Covered Computer System** by **You** or a third party service provider operating such **Covered Computer System** solely for **Your** benefit under a written agreement or contract with **You**; or
- (ii) the **Shared Computer System** by a third party service provider operating such **Shared Computer System** for **Your** benefit under a written agreement or contract with **You**,

which results in a loss, alteration or destruction of **Data**.

3.28 **Incident Response Expenses** means those reasonable expenses:

- A. to retain incident response management services for the purpose of coordinating response to a **Cyber Incident** or **Business Interruption Incident**;
- B. to retain the services of a third party computer forensics firm to determine the cause and scope of a **Cyber Incident** or **Business Interruption Incident**;
- C. to comply with consumer notification provisions of **Privacy Regulations** in the applicable jurisdiction that most favours coverage for such expenses, but only to the extent that such compliance is required because of a **Cyber Incident**, including but not limited to:
 - i. retaining the services of a notification or call centre support service; and
 - ii. retaining the services of a law firm to determine the applicability of and actions necessary to comply with **Privacy Regulations**;
- D. to retain a legal or regulatory advisor to handle and respond to any inquiries by any government agency, or functionally equivalent regulatory authority, alleging the violation of **Privacy Regulations**, including communicating with such government agency or functionally equivalent regulatory authority to determine the applicability and actions necessary to comply with **Privacy Regulations**, but not the costs to actually appear or defend **You** at a **Regulatory Proceeding**;
- E. to retain the services of a public relations firm, law firm or crisis management firm for advertising or related communications solely for the purpose of protecting or restoring **Your** reputation as a result of a **Cyber Incident** or **Business Interruption Incident**;
- F. to retain the services of a law firm solely to provide a preliminary legal opinion and advice as to **Your** rights and options with regards to the legal issues that arise as a result of the **Cyber Incident** or **Business Interruption Incident**, including determining **Your** potential indemnification rights under vendor contracts and preparing for and mitigating potential third party litigation;
- G. to retain the services of a licensed investigator or credit specialist to provide up to one year of fraud consultation to the individuals whose **Personal Data** has been wrongfully disclosed or otherwise compromised, and to retain a third party identity restoration service for those individuals who have been confirmed by such investigator or specialist as victims of identity theft resulting solely and directly from the **Cyber Incident**;
- H. for credit monitoring, identity theft monitoring, social media monitoring, credit freezing, fraud alert service or other fraud prevention software for those individuals whose **Personal Data** was wrongfully disclosed or otherwise compromised directly as a result of the **Cyber Incident**; and
- I. with **Our** prior consent (which shall not be unreasonably delayed or withheld):
 - i. to voluntarily notify individuals whose **Personal Data** has been wrongfully disclosed or otherwise compromised, including retaining a notification service or call centre support service; and
 - ii. any other reasonable expenses.

Incident Response Expenses shall not include:

- a) costs or expenses incurred to update or otherwise improve privacy or network security controls, policies or procedures to a level beyond that which existed prior to the **Cyber Incident** or **Business Interruption Incident** or to be compliant with **Privacy Regulations**, except to the extent **Betterment Costs** are applicable;
- b) taxes, fines, penalties, injunctions, or sanctions;

- c) **Regulatory Fines;**
- d) **Data and System Recovery Costs;**
- e) **Business Interruption Loss;**
- f) **Monies** or cryptocurrencies paid by **You** to terminate or end a **Cyber Extortion Event;**
- g) **Cyber Extortion Expenses;**
- h) **Your** wages, salaries, internal operating costs or expenses, or fees; or
- i) costs to respond to, commence or defend third party litigation related to the **Cyber Incident** or **Business Interruption Incident.**

3.29 **Indecent Content** means words, phrases, postings, pictures, advertisements or any other material that:

- A. is sexually explicit and is in violation of a statute prohibiting such content;
- B. is sexually explicit and posted without the consent of the natural person(s) depicted in the material;
- C. encourages, facilitates, incites, or threatens abuse, molestation, or sexual exploitation, including human trafficking and/or human sex trafficking; or
- D. encourages, facilitates, incites, or threatens physical violence, self-inflicted violence, or any other related harm, including terrorism.

3.30 **Infrastructure** means any of the following operated or supplied by a **Third Party**:

- A. electricity, gas, fuel, energy, water, telecommunications, or other utility;
- B. Internet infrastructure, including any Domain Name System (“DNS”), Certificate Authority, or Internet Service Provider (“ISP”);
- C. satellite; or
- D. financial transaction or payment process platform, including a securities exchange.

3.31 **Insurance Representative** means the person(s) employed by the **Insured Organisation** who is responsible for procuring and maintaining the **Insured Organisation's** insurance policy(ies).

3.32 **Insured** means the **Insured Organisation** and any **Insured Person**.

3.33 **Insured Organisation** means the **Named Insured** and any **Subsidiary**.

3.34 **Insured Person** means:

- A. any past, present or future principal, partner, officer, director, trustee, supervisory board member, employee, leased employee, or temporary employee of the **Insured Organisation** while acting on the **Insured Organisation's** behalf or at the **Insured Organisation's** direction and control;
- B. independent contractors of the **Insured Organisation**, who are natural persons, whilst performing duties on behalf of the **Insured Organisation**.

The term **Insured Person** also includes:

- i. any domestic partner of a principal, partner, director, officer, trustee or employee, but only where the third party claim which would have been covered under this **Policy** if brought against the principal, partner, director, officer, trustee or employee, is brought against such domestic partner; and
- ii. the estate, heir or legal representative of a deceased principal, partner, director, officer, trustee or employee, but only where the third party claim which would have been covered under this **Policy** if brought against such principal, partner, director, officer, trustee or employee, is brought against such estate, heir or legal representative.

The term **Insured Person** does not include any auditor, receiver, liquidator, administrator, trustee in bankruptcy, mortgagee in possession or any employees of such person.

- 3.35 **Insurer** means Chubb Insurance Australia Limited (ABN: 23 001 642 020, AFSL: 239687).
- 3.36 **Loss** means any **Damages** or **Expenses**.
- 3.37 **Malicious Use or Access** means:
- A. the prohibited, unlawful and unauthorised entry to, use or access of a **Covered Computer System** or a **Shared Computer System**; or
 - B. the prohibited, unlawful and unauthorised entry to, use or access of a **Covered Telecom System** or a **Shared Telecom System**.
- 3.38 **Media Claim** means:
- A. a demand against **You** for monetary or non-monetary damages;
 - B. a civil proceeding against **You** seeking monetary damages or non-monetary or injunctive relief, commenced by the service of a complaint or similar pleading; or
 - C. an arbitration proceeding against **You** seeking monetary damages or non-monetary or injunctive relief.
- 3.39 **Media Claims Expenses** means:
- A. reasonable legal fees, expert witness fees and other fees and costs incurred by **Us**, or by **You** with **Our** prior consent, such consent not to be unreasonably withheld or delayed, in the investigation and defence of a covered **Media Claim**;
 - B. reasonable premiums for any appeal bond, attachment bond or similar bond, provided that **We** shall have no obligation to apply for or furnish such bond; and
 - C. subject to **Our** prior approval (which shall not be unreasonably withheld or delayed), reasonable fees incurred for public relations and crisis communications services.
- 3.40 **Media Content** means electronic media distributed by or on behalf of **You** on the internet, including on social media websites.
- 3.41 **Media Services** means the publication, distribution, or broadcast of **Media Content**.
- 3.42 **Media Wrongful Act** means any actual or alleged:
- A. disparagement or harm to the reputation or character of any person or organisation, defamation, libel, slander, product disparagement, trade libel, infliction of emotional distress, mental anguish and injurious falsehood;
 - B. eavesdropping, false arrest or malicious prosecution;
 - C. plagiarism, piracy or misappropriation of ideas in connection with any **Media Content**;
 - D. infringement of copyright, domain name, trade dress, title or slogan, or the dilution or infringement of trademark, service mark, service name or trade name; but not actual or alleged infringement of any patent or **Trade Secret**; or
 - E. negligence with respect to the **Insured's** creation or dissemination of **Media Content**;
- committed by the **Insured** solely in the performance of providing **Media Services**.
- Media Wrongful Act** shall not include any kind of discrimination or discriminatory conduct, including any alleged **Media Claims** of unequal or complete lack of access to **Your** website and/or **Media Content**.

- 3.43 **Money or Monies** means currency, coins, bank notes, bullion, cheques, travellers cheques, registered cheques, postal orders, money orders held for sale to the public or funds, whether in physical or held via electronic means.
- Money** does not include cryptocurrencies, goods or tangible property.
- 3.44 **Named Insured** means the organisation first specified in Item 1 of the **Schedule**.
- 3.45 **Natural Person** means an individual who can be identified by specific reference to an identifier such as a name, national identification number or other government issued identification number, location data, an online identifier such as an IP address, or by one or more factors specific to the physical, cultural or social identity of that individual.
- 3.46 **Neglected Software Exploit** means the exploitation of a vulnerability in software, where, as of the first known date of exploitation:
- A. such software has been withdrawn, is no longer available, is no longer supported by, or has reached end-of-life or end-of-support status with the vendor that developed it, and where extended support from such vendor has no longer been purchased; or
 - B. such vulnerability has been listed as a Common Vulnerability and Exposure (a “CVE”) and a Common Vulnerability Scoring System (“CVSS”) score of 7.0 or above has been assigned in the National Vulnerability Database, operated by the National Institute of Standards and Technology, and a patch, fix, or mitigation technique for such vulnerability has been available to **You**, but has not been applied by such **Insured**,
- for the applicable number of days shown as ranges in the Additional Sub-Limits section for **Neglected Software Exploit** set forth in Item 3 of the **Schedule**.
- 3.47 **Net Profit** means the operating profit resulting from **Your** business after a deduction has been made for all fixed charges. Such fixed charges include **Your** continuing operating and payroll expenses, considering any cost savings.
- 3.48 **Network Security** means those activities performed by **You**, or by others on behalf of **You**, to protect against **Computer Malicious Acts** or **Unauthorised Use or Access**.
- 3.49 **Payment Card Loss** means monetary assessments, fines, penalties, chargebacks, reimbursements, and fraud recoveries that **You** become legally obligated to pay as a result of a **Privacy and Network Security Wrongful Act** and where such amount is due to **Your** non-compliance with the Payment Card Industry Data Security Standard.
- Payment Card Loss** shall not include:
- A. subsequent fines or monetary assessments for continued noncompliance with the Payment Card Industry Data Security Standard beyond a period of three months from the date of the initial fine or monetary assessment; or
 - B. costs or expenses incurred to update or otherwise improve privacy or network security controls, policies or procedures.
- 3.50 **Period of Indemnity** means the period stated at Item 7 of the **Schedule** during which **You** incur **Business Interruption Loss** or **Data and System Recovery Costs**, beginning when the **Business Interruption Incident** occurs.
- 3.51 **Personal Data** means:
- A. a **Natural Person's** name, national identity number or national insurance number, medical or healthcare data, other protected health information, driver's license number, state identification number, credit card number, debit card number, address, telephone number, email address, account number, account histories, or passwords; and
 - B. any other protected personal information as defined in **Privacy Regulations**;

in any format.

- 3.52 **Personal Injury** means injury arising out of one or more of the following offences:
- A. false arrest, detention or imprisonment;
 - B. malicious prosecution;
 - C. libel, slander, or other defamatory or disparaging material;
 - D. publication or an utterance in violation of an individual's right to privacy; and
 - E. wrongful entry or eviction, or other invasion of the right to private occupancy.
- 3.53 **Policy** means, collectively, the **Schedule**, the proposal, this policy form and any endorsements.
- 3.54 **Policy Aggregate** means the amount stated as such in the **Schedule** which is the maximum aggregate amount payable by **Us** under the **Policy** in respect of the **Policy Period** irrespective of the number of **Claims**, the number of Sub-Limits, the number of **Aggregate Limits**, number of claimants, number of **Insureds** making a **Claim**, number of Insuring Agreements and/or Insuring Agreement Extensions claimed under and/or any combination of those things.
- 3.55 **Policy Period** means the period of time specified in Item 2 of the **Schedule**, subject to any applicable prior termination pursuant to Section 5, General Conditions.
- 3.56 **Pollutants** means any solid, liquid, gaseous or thermal irritant or contaminant, including smoke, vapour, soot, fumes, acids, alkalis, chemicals, asbestos, asbestos products or waste (waste includes materials to be recycled, reconditioned or reclaimed).
- 3.57 **Privacy and Network Security Claim** means:
- A. a demand against **You** for monetary or non-monetary damages;
 - B. a civil proceeding against **You** seeking monetary damages or non-monetary or injunctive relief, commenced by the service of a complaint or similar pleading;
 - C. an arbitration proceeding against **You** seeking monetary damages or non-monetary or injunctive relief; and
 - D. a **Regulatory Proceeding**.
- 3.58 **Privacy and Network Security Claims Expenses** means:
- A. reasonable legal fees, expert witness fees and other fees and costs incurred by **Us**, or by **You** with **Our** prior consent (which shall not be unreasonably delayed or withheld), in the investigation and defence of a covered **Privacy and Network Security Claim**; and
 - B. reasonable premiums for any appeal bond, attachment bond or similar bond, provided **We** shall have no obligation to apply for or furnish such bond.
- 3.59 **Privacy and Network Security Wrongful Act** means any actual or alleged:
- A. failure of **Network Security**, including the failure to deter, inhibit, defend against or detect any **Computer Malicious Act** or **Unauthorised Use or Access**, including that which causes **Personal Injury**;
 - B. failure by **You** or by an independent contractor for which **You** are legally responsible to handle, manage, store, destroy or otherwise control:
 - i. **Personal Data**, including that which causes **Personal Injury**; or

ii. Non-public, private third party corporate information in any format provided to **You**;
or

C. unintentional violation of **Your** privacy policy that results in the violation of any **Privacy Regulation**, including but not limited to the unintentional wrongful use or collection of **Personal Data** by **You**.

3.60 **Privacy Regulations** means regulations applying to the care, collection, custody, control, use, or disclosure of **Personal Data**, including **Data** that is regulated by the General Data Protection Regulation (GDPR).

3.61 **Products** means anything that the **Insured** sells, designed, created, developed, assembled, manufactured, handled, installed, disposed of, leased to or licensed for others, sold, or that is distributed by or on behalf of an **Insured**, including the repair or maintenance of such things.

3.62 **Programming Error** means an error:

A. by **You** or by a third party service provider operating a **Covered Computer System** solely for **Your** benefit under a written agreement or contract with **You**, that occurs during the development or encoding of a program, application or operating system on a **Covered Computer System** that would, once in operation, result in a malfunction of and/or an interruption of operation and/or an incorrect result of such **Covered Computer System**;

B. by a third party service provider operating a **Shared Computer System** for **Your** benefit under a written agreement or contract with **You**, that occurs during the development or encoding of a program, application or operating system on a **Shared Computer System**, that would, once in operation, result in a malfunction and/or an interruption of operation and/or an incorrect result of such **Shared Computer System**.

Programming Error does not include integration, installation, upgrade or patching of any software, hardware or firmware on a **Covered Computer System** or a **Shared Computer System** unless **You** can provide proof that the **Programming Error** arises from an **Accepted Program**.

3.63 **Property Damage** means physical injury to or loss or destruction of tangible property, including the loss of use of such property. **Property Damage** shall not include any injury to, loss or destruction of, or loss of use of **Data**.

3.64 **Ransomware** means any any extortive demand of **Money** or cryptocurrency(ies) from **You** in connection with a:

A. **Cyber Incident** and/or **Business Interruption Incident** and/or **Cyber Extortion Event** and/or **Privacy and Network Security Wrongful Act** that involves malicious software which is designed to block access to a **Computer System** or data, or alter, corrupt, damage, manipulate, misappropriate, encrypt, delete, or destroy data; and/or

B. credible threat, or series of credible connected threats, to release, divulge, disseminate, or use such data that has been exfiltrated as part of an event described in paragraph (A) immediately above.

3.65 **Regulatory Fines** means any civil monetary fine or penalty imposed by a government or regulatory body, including an official governmental entity in such entity's regulatory or official capacity pursuant to its order under a **Regulatory Proceeding**. **Regulatory Fines** shall not include any civil monetary fines or penalties that are not insurable by law, criminal fines, disgorgement of profits or multiple damages.

3.66 **Regulatory Proceeding** means a request for information, demand, suit, civil investigation or civil proceeding by or on behalf of a government agency, commenced by a service of a complaint or similar pleading alleging the violation of **Privacy Regulations** as a result of **Your Privacy and Network Security Wrongful Act** and that may reasonably be expected to give rise to a covered **Privacy and**

Network Security Claim under Insuring Agreement 1.5 of this **Policy**. Additionally, **Regulatory Proceeding** does not include any action, proceeding or suit, or the portion of any action, proceeding or suit, that is based on or related to a criminal violation of **Privacy Regulations**.

3.67 **Retroactive Date** means the date specified in Item 4 of the **Schedule**.

3.68 **Reward Expenses**, applicable to Insuring Agreement Extension 2.4 only, means the reasonable amount of money or other security paid by an **Insured Organisation**, with **Our** prior consent which will not be unreasonably withheld, to a third party natural person, who is not affiliated with or employed by the **Insured Organisation**, and who provides information not otherwise available that leads to the arrest and conviction of any person responsible for the **Cyber Extortion Event**.

Reward Expenses shall not include any **Emergency Incident Response Expenses**, **Incident Response Expenses** or **Cyber Extortion Expenses**.

Reward Expenses shall be a part of and not in addition to the applicable **Aggregate Limit** shown in the **Schedule** for Cyber Extortion as provided for under Insuring Agreement 1.4, and shall reduce such applicable **Aggregate Limit**.

3.69 **Schedule** means the schedule attached to this **Policy**.

3.70 **Securities**, applicable to Insuring Agreement Extension 2.3 only, means negotiable and non-negotiable instruments or contracts, including any note, stock, bond, debenture, evidence of indebtedness, share or other equity or debt security, representing either money or property, but does not include **Money** or cryptocurrencies. **Securities** also does not include goods or tangible property.

3.71 **Shared Computer System** means a **Computer System**, other than a **Covered Computer System**, operated for **Your** benefit, by a **Third Party** under a written agreement or contract with **You** to provide data hosting, cloud services or computing, co-location, data back-up, data storage, data processing, platforms-as-a-service, software-as-a-service, infrastructure-as-a-service, or any similar type of outsourced computing services. However, **Shared Computer System** shall not include **Infrastructure**.

3.72 **Shared Telecom System** means a fixed line telecom system operated for **Your** benefit by a **Third Party** under a written agreement or contract with **You**. However, **Shared Telecom System** shall not include **Infrastructure**.

3.73 **Single Claim** means all **Claims** or other matters giving rise to a claim under this **Policy** that relate to the same originating source or cause or the same underlying source or cause, regardless of whether such **Claims**, **Regulatory Proceedings** or other matters giving rise to a claim under this **Policy** involve the same or different claimants, **Insureds**, events, or legal causes of action.

3.74 **Subsidiary** means any entity that is not formed as a partnership or joint venture in which, at the inception of the **Policy**, the **Named Insured** directly or indirectly:

- A. holds more than 50% of the voting rights;
- B. has the right to appoint or remove more than 50% of the board of directors; or
- C. controls alone, pursuant to a written agreement with other shareholders, more than 50% of the voting rights.

If a **Subsidiary** ceases to be a **Subsidiary** either prior to or during the **Policy Period**, this **Policy** shall continue to cover such **Subsidiary** and its **Insured Persons**, but:

- i. only for **Privacy and Network Security Wrongful Acts** and **Media Wrongful Acts** that occur after the **Retroactive Date** and while the entity was a **Subsidiary**; and
- ii. only for **Cyber Incidents**, **Business Interruption Incidents**, **Cyber Extortion Events**, and **Theft** discovered by any **Control Group** member while the entity was a **Subsidiary**.

- 3.75 **Telecom Data** means any software or other information in electronic form which is stored on a **Covered Telecom System** or a **Shared Telecom System**. **Telecom Data** includes any information or programs that allow a **Covered Telecom System** or a **Shared Telecom System** and any of their accessories to function, including systems and applications software, hard or floppy disks, CD-ROMs, tapes, drives, cells, data processing devices or any other media that are used with electronically controlled equipment or other electronic backup facilities.
- Telecom Data** does not constitute the actual hardware or tangible property.
- 3.76 **Telecom Malicious Act** means any malicious act committed against a **Covered Telecom System** or a **Shared Telecom System** or malicious access to or hacking of a **Covered Telecom System** or **Shared Telecom System**, for the purpose of creating, deleting, taking, collecting, altering or destroying **Telecom Data** or services.
- Telecom Malicious Act** includes a distributed denial of service attack or the introduction of malicious code, ransomware, cryptoware, virus, trojans, worms and logic or time bombs or any malware, programs, files or instructions of a malicious nature which may disrupt, harm, impede access to, or in any other way corrupt the operation of a **Covered Telecom System**, a **Shared Telecom System**, **Telecom Data** or software within.
- 3.77 **Telecommunications Expenses**, applicable to Insuring Agreement Extension 2.5 only, means the amount invoiced for unauthorised voice or data charges or unauthorised bandwidth.
- Telecommunications Expenses** shall not include any fraudulent charges waived, reimbursed, or recovered by or on behalf of the telecommunications provider. Additionally, **Telecommunications Expenses** shall not include any voice, data or bandwidth charges incurred because of the intentional, negligent or wrongful misuse or overuse of a **Covered Telecom System** or a **Shared Telecom System** by employees or authorised third parties, who have legitimate access to a **Covered Telecom System** or a **Shared Telecom System**.
- 3.78 **Theft**, applicable to Insuring Agreement Extension 2.3 only, means a dishonest and unlawful act of a **Third Party** of taking **Your Money** or **Your Securities** with the intention of permanently depriving **You** of its use.
- 3.79 **Third Party** means an entity or natural person not qualifying as an **Insured** under this **Policy**.
- 3.80 **Trade Secret** means information, including a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable by other persons who can obtain value from its disclosure or use, so long as reasonable efforts have been made to maintain its secrecy.
- 3.81 **Transaction** means in respect of the company shown in Item 1 of the **Schedule**:
- A. it or all of its assets is or are acquired by another entity;
 - B. it merges or consolidates into or with another entity;
 - C. any person, entity or affiliated group of persons and/or entities obtains the right or power to elect, appoint or designate at least fifty percent (50%) of the directors of it;
 - D. any person, entity or affiliated group of persons and/or entities acquires fifty percent (50%) or more of the issued capital of it; or
 - E. a receiver, receiver and manager, liquidator, administrator, official manager or trustee is appointed to manage, administer, liquidate, supervise, or otherwise take control.
- 3.82 **Unauthorised Use or Access** means the entry or access to a **Covered Computer System** or a **Shared Computer System** by an unauthorised party or individual, including an employee or authorised party acting outside the scope of their authority.

- 3.83 **Waiting Period** means the number of hours specified in Item 3 (Business Interruption) of the **Schedule** following a **Business Interruption Incident**.
- 3.84 **We, Us, and Our** means the **Insurer**.
- 3.85 **Wrongful Act** means an actual or alleged **Privacy and Network Security Wrongful Act, Media Wrongful Act, Malicious Use or Access, Cyber Incident, Cyber Extortion Event** or **Business Interruption Incident**.
- 3.86 **Wrongful Employment Practices** means any actual or alleged violation of employment laws or any other legal provisions relating to any individual's actual or prospective employment relationship with the **Insured**, including:
- A. employment-related invasion of privacy, except with respect to that part of any **Privacy and Network Security Claim** arising out of the loss of **Personal Data** that is otherwise covered under Insuring Agreement 1.5 of this **Policy**; and
 - B. employment-related wrongful infliction of emotional distress, except with respect to that part of any **Privacy and Network Security Claim** arising out of the loss of **Personal Data** that is otherwise covered under Insuring Agreement 1.5 of this **Policy**.
- 3.87 **You and Your** means the **Insured**.

4A. Exclusions Applicable to Definitions (Section 3)

Certain defined terms in the Definitions section of this **Policy** contain exclusions that change, limit or reduce cover under this **Policy**. The exclusions contained in those defined terms are listed below:

4A.1 *Bodily Injury*

Bodily Injury (General Definitions section 3.4) does not include any mental injury, mental anguish, mental tension, emotional distress, pain and suffering, or shock that arises out of a **Privacy and Network Security** or **Media Wrongful Act** as expressly covered under Insuring Agreements 1.5 or 1.6.

4A.2 *Business Interruption Loss*

Business Interruption Loss (General Definitions section 3.6) does not include amounts that accrued during the **Waiting Period**.

4A.3 *Consumer Redress Fund*

Consumer Redress Fund (General Definitions section 3.11) shall not include any sums paid which constitute taxes, fines, penalties, injunctions or sanctions.

4A.4 *Cyber Extortion Event*

Cyber Extortion Event (General Definitions section 3.16) shall not include any threats or connected series of threats made against **You** expressing intent to perform or cause any of the above if made, approved or directed by a member of the **Control Group**.

4A.5 *Damages*

Damages (General Definitions section 3.19) shall not include:

- a) any amount for which **You** are not legally obligated to pay; matters uninsurable under the laws pursuant to which this **Policy** is construed;

the cost to comply with any injunctive or other non-monetary or declaratory relief, including specific performance, or any agreement to provide such relief;
You loss of fees or profits, return of fees, commissions;
royalties, or re-performance of services by **You** or under **Your** supervision;
disgorgement of any profit, remuneration or financial advantage to which **You** are not legally entitled;
any amounts other than those which compensate solely for a loss caused by a **Wrongful Act**, unless specifically provided for in this **Policy**.

With respect to Insuring Agreement 1.5, **Damages** shall not include any amounts owed or paid by or to an **Insured**, which arise solely under a contract or agreement to the extent they exceed the amount for which **You** would otherwise be liable for in absence of the contract or agreement, including any royalties, restitution, reduction, disgorgement or return of any payment, charges, or fees; or costs to correct or re-perform services related to **Products**, including for the recall, loss of use, or removal of **Products**.

4A.6 *Data*

Data (General Definitions section 3.20) shall not include or be considered tangible property.

4A.7 *Data and System Recovery Costs*

Data and System Recovery Costs (General Definitions section 3.21) do not include:

- a) costs or expenses incurred to identify or remediate software vulnerabilities;
- b) costs to replace any hardware or physical property;
- c) costs incurred to research and develop **Data**, including **Trade Secrets**;
- d) the economic or market value of **Data**, including **Trade Secrets**;
- e) any other loss or damage which does not result directly from the **Business Interruption Incident**;
- f) **Incident Response Expenses**; or
- g) costs to update, upgrade, replace, maintain, or improve any **Data** or **Computer System** beyond what is provided in 3.21, D, (i) and (ii).

4A.8 *Incident Response Expenses*

Incident Response Expenses (General Definitions section 3.28) shall not include:

- (a) costs or expenses incurred to update or otherwise improve privacy or network security controls, policies or procedures to a level beyond that which existed prior to the **Cyber Incident** or **Business Interruption Incident** or to be compliant with **Privacy Regulations**, except to the extent **Betterment Costs** are applicable;
- (b) taxes, fines, penalties, injunctions, or sanctions;
- (c) **Regulatory Fines**;
- (d) **Data and System Recovery Costs**;
- (e) **Business Interruption Loss**;
- (f) **Monies** or cryptocurrencies paid by **You** to terminate or end a **Cyber Extortion Event**;
- (g) **Cyber Extortion Expenses**;
- (h) **Your** wages, salaries, internal operating costs or expenses, or fees; or
- (i) costs to respond to, commence or defend third party litigation related to the **Cyber Incident** or **Business Interruption Incident**.

Incident Response Expenses also do not include the costs to actually appear or defend **You** at a **Regulatory Proceeding**.

4A.9 *Media Wrongful Act*

Media Wrongful Act (General Definitions section 3.42) shall not include any kind of discrimination or discriminatory conduct, including any alleged **Media Claims** of unequal or complete lack of access to **Your** website and/or **Media Content**.

4A.10 *Money*

Money (General Definitions section 3.43) does not include cryptocurrencies, goods or tangible property.

4A.11 *Payment Card Loss*

Payment Card Loss (General Definitions section 3.49) shall not include:

- a) subsequent fines or monetary assessments for continued noncompliance with the Payment Card Industry Data Security Standard beyond a period of three months from the date of the initial fine or monetary assessment; or
- b) costs or expenses incurred to update or otherwise improve privacy or network security controls, policies or procedures.

4A.12 *Programming Error*

Programming Error (General Definitions section 3.62) does not include integration, installation, upgrade or patching of any software, hardware or firmware on a **Covered Computer System** or a **Shared Computer System** unless **You** can provide proof that the **Programming Error** arises from an **Accepted Program**.

4A.13 *Property Damage*

Property Damage (General Definitions section 3.63) shall not include any injury to, loss or destruction of, or loss of use of **Data**.

4A.14 *Regulatory Fines*

Regulatory Fines (General Definitions section 3.65) shall not include any civil monetary fines or penalties that are not insurable by law, criminal fines, disgorgement of profits or multiple damages.

4A.15 *Regulatory Proceeding*

Regulatory Proceeding (General Definitions section 3.66) does not include any action, proceeding or suit, or the portion of any action, proceeding or suit, that is based on or related to a criminal violation of **Privacy Regulations**.

4A.16 *Reward Expenses*

Reward Expenses (General Definitions section 3.68) shall not include any **Emergency Incident Response Expenses**, **Incident Response Expenses** or **Cyber Extortion Expenses**.

4A.17 *Securities*

Securities (General Definitions section 3.70) shall not include **Money**, cryptocurrencies, goods or tangible property.

4A.18 *Shared Computer System*

Shared Computer System (General Definitions section 3.71) shall not include **Infrastructure**.

4A.19 *Shared Telecom System*

Shared Telecom System (General Definitions section 3.72) shall not include **Infrastructure**.

4A.20 *Telecommunications Expenses*

Telecommunications Expenses (General Definitions section 3.77) shall not include any fraudulent charges waived, reimbursed, or recovered by or on behalf of the telecommunications provider. Additionally, **Telecommunications Expenses** shall not include any voice, data or

bandwidth charges incurred because of the intentional, negligent or wrongful misuse or overuse of a **Covered Telecom System** or a **Shared Telecom System** by employees or authorised third parties, who have legitimate access to a **Covered Telecom System** or a **Shared Telecom System**.

4. General Exclusions

We shall not be liable for **Loss** on account of any **Claim**:

4.1 *Prior Knowledge*

alleging, based upon, arising out of or attributable to a **Wrongful Act** actually or allegedly committed prior to the beginning of the **Policy Period** if, on or before the earlier of the effective date of this **Policy** or the effective date of any **Policy** issued by **Us** of which this **Policy** is a continuous renewal or a replacement, any member of the **Control Group** of the **Insured** knew or reasonably could have foreseen that the **Wrongful Act** did or could lead to any **Loss**.

4.2 *Pending or Prior Proceedings*

alleging, based upon, arising out of, or attributable to:

- A. any prior or pending litigation, **Privacy and Network Security Claim, Media Claim**, demand, arbitration, administrative or regulatory proceeding or investigation filed or commenced against **You**, and of which **You** had notice, on or before the earlier of the effective date of this **Policy** or the effective date of any policy issued by **Us** of which this **Policy** is a continuous renewal or a replacement, or alleging or derived from the same or substantially the same fact, circumstance or situation underlying or alleged therein; or
- B. any **Wrongful Act**, fact, circumstance or situation that has been the subject of any notice given under any other policy before the effective date of this **Policy** or any other **Wrongful Act** whenever occurring which, together with a **Wrongful Act** that has been the subject of such notice, would constitute a **Single Claim**.

4.3 *Conduct*

directly or indirectly caused by, arising out of or in any way connected with **Your** conduct, or of any person for whose conduct **You** are legally responsible, that involves:

- A. committing or permitting any knowing or willful breach of duty, or willful violation, of any laws; or
- B. committing or permitting any criminal, deliberately fraudulent or deliberately dishonest act or failure to act; or
- C. any actual or attempted gain of personal profit, secret profit or advantage by **You** to which **You** were not entitled.
- D. the intentional unauthorised, surreptitious, or wrongful use or collection of **Personal Data** by **You**.

This exclusion only applies where such conduct has been established to have occurred by final adjudication (after the exhaustion of any appeals), or written admission.

Conduct committed by an **Insured Person** shall not be imputed to any other **Insured Person** or to an **Insured Organisation**. However, conduct committed by or with the knowledge of a past, present, or future member of the **Control Group** shall be imputed to the relevant **Insured Organisation**.

4.4 *Discrimination or Employment Practices*

alleging, based upon, arising out of or attributable to any:

- A. discrimination of any kind; or
- B. humiliation, harassment or misconduct based upon, arising out of or related to any such discrimination; or
- C. **Wrongful Employment Practices.**

However, this exclusion shall not apply with respect to that part of any **Privacy and Network Security Claim** alleging employment-related invasion of privacy or employment-related wrongful infliction of emotional distress in the event such **Privacy and Network Security Claim** arises out of the loss of **Personal Data** which is covered under Insuring Agreement 1.5.

4.5 *Insured v. Insured*

brought or maintained by **You**, or on **Your** behalf, or any other natural person or entity for whom or which **You** are legally liable, arising out of a **Privacy and Network Security Claim** or **Media Claim**. However, this exclusion shall not apply to a **Privacy and Network Security Claim** brought against **You** by an **Insured Person**, alleging that **You** committed a **Privacy and Network Security Wrongful Act** as outlined in parts B and C only, which is expressly covered under Insuring Agreement 1.5.

4.6 *Contract*

for breach of any express, implied, actual or constructive contract, warranty, guarantee, or promise, including liquidated damages provisions or any liability assumed by **You**. This exclusion shall not apply to:

- A. any liability or obligation **You** would have in the absence of such contract, warranty, promise or agreement; or
- B. any indemnity by **You** in a written contract or agreement with **Your** client regarding any **Privacy and Network Security Wrongful Act** that results in the failure to preserve the confidentiality or privacy of **Personal Data** of customers of **Your** client; or
- C. with respect to Insuring Agreement 1.5, any **Payment Card Loss**.

4.7 *Fees*

solely with respect to coverage under Insuring Agreements 1.5 and 1.6, alleging, based upon, arising out of or attributable to any fees, expenses, or costs paid to or charged by **You**.

4.8 *Bodily Injury and Property Damage*

alleging, based upon, arising out of or attributable to any **Bodily Injury** or **Property Damage**.

4.9 *Infrastructure*

alleging, based upon, arising out of or attributable to any failure, interruption, disturbance, degradation, corruption, impairment, or outage of **Infrastructure**.

4.10 *Natural Perils*

alleging, based upon, arising out of or attributable to fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption, electromagnetic pulse or radiation, tidal wave, landslide, hail, natural weather or seismic event or any other natural physical event, however caused.

4.11 *War*

alleging, based upon, arising out of or attributable to:

- A. any **Computer Malicious Act** and/or **Unauthorised Use or Access** committed, in whole or in part, by or on behalf of a sovereign State or state-sponsored actor that results in or is cited as a reason:
 - i. in a G7 (Group of Seven) Leader or any governmental body of any other sovereign State ordering actions that constitute the use of force against a sovereign State;
 - ii. in a resolution or other formal action by the United Nations Security Council authorising the use of force or economic sanctions against a sovereign State, or that results in the use of force by the North Atlantic Treaty Organization or any other equivalent international intergovernmental military or political alliance, against a sovereign State;
- B. any hostile act, or series of similar or related acts, committed, in whole or in part, by or on behalf of a sovereign State or state-sponsored actor:
 - i. that results in or is cited as a reason in a formal declaration of war by any responsible governmental body of any other sovereign State against a sovereign State;
 - ii. following any of the events described in paragraphs A and B(i) above, where such hostile act has the same originating source or cause or the same underlying source or cause as the **Computer Malicious Act** and/or **Unauthorised Use or Access** and/or hostile act described in paragraphs A and B(i) above; or
- C. civil war, rebellion, revolution or insurrection.

4.12 *Pollution*

alleging, based upon, arising out of or attributable to the actual, alleged or threatened discharge, release, escape, seepage, migration, or disposal of **Pollutants**, or any direction, formal mandate or request that any **Insured** test for, monitor, clean up, remove, contain, treat, detoxify or neutralise **Pollutants**, or any voluntary decision to do so.

4.13 *Wear and Tear*

solely with respect to coverage under Insuring Agreements 1.1, 1.2 and 1.3, and Insuring Agreement Extensions 2.1, 2.2 and 2.5, alleging, based upon, arising out of, or attributable to the ordinary wear and tear or gradual deterioration of a **Covered Computer System, Shared Computer System, Covered Telecom System, Shared Telecom System, Data or Telecom Data**, including any data processing media.

4.14 *Patent and Trade Secret*

alleging, based upon, arising out of or attributable to any claim, dispute or issues with the validity, invalidity, infringement, violation or misappropriation of any patent or **Trade Secret** by or on behalf of **You**.

4.15 *Intellectual Property*

alleging, based upon, arising out of or attributable to any infringement, violation or misappropriation by **You** of any copyright, service mark, trade name, trademark or other intellectual property of any third party. However, this exclusion shall not apply to a **Privacy and Network Security Wrongful Act** or **Media Wrongful Act** expressly covered under Insuring Agreements 1.5 or 1.6.

4.16 *Advertising or Misrepresentation*

Solely with respect to coverage under Insuring Agreement 1.6, alleging, arising out of, or attributable to the actual goods, **Products** or services described, illustrated or displayed in **Media Content**.

4.17 *Products*

alleging, based upon, arising out of or attributable to any **Products**.

4.18 *Trading*

alleging, based upon, arising out of or attributable to any:

- A. financial loss due to the inability to trade, invest, divest, buy or sell any financial security or financial asset of any kind;
- B. fluctuations in any value of assets;
- C. financial value in any of **Your** accounts held at a financial institution; or
- D. inability to earn interest or appreciation on any asset.

4.19 *Cyber Crime*

solely with respect to coverage under Insuring Agreement Extension 2.3, **We** will not pay for **Direct Financial Loss** consisting of or which is due to:

- A. any acts by employees or independent contractors of the **Insured**, including any such acts caused by collusion with an employee or independent contractor;
- B. any acts by directors, executive officers or executive managers of the **Insured**, including any such acts caused by collusion with a director, executive officer or executive manager;
- C. any government seizures of **Your Money** or **Securities**;
- D. any fluctuation in value in any **Monies** or **Securities**;
- E. any other loss or damage which does not result directly from the **Direct Financial Loss**;
- F. recall costs or expenses.

4.20 *Government Authority*

alleging, based upon, arising out of or attributable to any public or governmental authority, foreign enemy, military, or usurped power:

- A. seizing or confiscating a **Covered Computer System**, a **Shared Computer System**, a **Covered Telecom System**, a **Shared Telecom System**, **Data** or **Telecom Data**; and/or
- B. mandating the restriction of operations, closure, or shutdown of:
 - i. any entity or person operating a **Computer System**; and/or
 - ii. any **Computer System**;

However, this Exclusion shall not apply to any such actions of a public or governmental authority directed solely against a **Covered Computer System** or **Covered Telecom System** in response to a **Computer Malicious Act**, **Unauthorised Use or Access**, **Telecom Malicious Act** or **Malicious Use or Access** also directed solely against such **Covered Computer System** or **Covered Telecom System**.

4.21 *Antitrust or Unfair Trade Practices*

alleging, based upon, arising out of or attributable to any price fixing, restraint of trade, monopolization, interference with economic relations (including interference with contractual relations or with prospective advantage), unfair competition, unfair business or unfair trade practices, including any violation of the Federal Trade Commission Act, the Sherman Anti-Trust Act, the Clayton Act, or any other federal and/or state statutory provision involving anti-trust, monopoly, price fixing, price discrimination, predatory pricing, restraint of trade, unfair competition, unfair business or unfair trade practices, and any amendments to such Acts or statutes or any rules or regulations made under such Acts or statutes, amendments to such rules or regulations, or any similar federal, state, or common law anywhere in the world.

However, solely with respect to Insuring Agreement 1.5, this exclusion shall not apply to a **Privacy and Network Security Claim** resulting directly from a violation of a **Privacy Regulation**.

4.22 *Communications Decency*

alleging, based upon, arising out of or attributable to the failure of **You**, or others for whom **You** are legally responsible, to prevent the publication or dissemination of **Indecent Content**.

4.23 *Contest or Game of Chance*

solely with respect to the Insuring Agreement for Media Liability, alleging, based upon, arising out of, or attributable to any gambling, contest, game of chance or skill, lottery, or promotional game, including tickets or coupons or over-redemption related to the same.

4.24 *Inaccurate Price, Cost or Estimates*

solely with respect to the Insuring Agreements for Privacy and Network Security Liability and Media Liability, **Your** cost guarantees, cost representations, contract price, pricing guarantees, or estimates of probable costs or cost estimates being exceeded, or any guarantee or promise of cost savings, return on investment, or profitability.

4.25 *Violations of specified United States statutes*

alleging, based upon, arising out of or attributable to:

- (i) any **Claim** brought within the United States of America in respect of the following; or
- (ii) based upon any action or liability originating in the United States of America out of the following:

A. Consumer Protection Laws: any violation by an **Insured** of the Truth in Lending Act, Fair Debt Collection Practices Act, or the Fair Credit Reporting Act or any amendments to those Acts or any rules or regulations made under those Acts, including the Fair and Accurate Credit Transactions Act, and any amendments to such Act or any rules or regulations made under such Act, amendments of such Acts, or any similar federal, state or common law. However, solely with respect to Insuring Agreement 1.5, this exclusion shall not apply to a **Privacy and Network Security Claim** arising out of the actual or alleged disclosure or theft of **Personal Data** resulting from a **Privacy and Network Wrongful Act**.

B. ERISA or Securities Law: an Insured's violation of:

- i. the Employee Retirement Income Security Act of 1974;
- ii. the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940;
- iii. the Investment Advisors Act, or any other federal, state or local securities law;

and any amendments to those Acts or any rules or regulations made under those Acts, amendments of those rules or regulations, or any similar federal, state or common law. However, with respect to Insuring Agreements 1.1 (Incident Response) or 1.5 (Privacy and Network Security Liability), paragraph i, immediately above, shall not apply.

- C. **Unsolicited Communications:** any unsolicited electronic dissemination of faxes, emails or other communications by or on behalf of an **Insured**, including actions brought under the Telephone Consumer Protection Act and any rules or regulations made under such Act, any federal or state anti-spam statutes, or any other federal or state statute, law, rule, regulation or common law relating to a person's or entity's right of seclusion and any amendments to such Act or to any state statute, law, rule, regulation or common law. However, with respect to Insuring Agreement 1.5 (Privacy and Network Security Liability), this exclusion shall not apply to a **Privacy and Network Security Claim** resulting from an act as defined under subparagraph C of the definition of **Privacy and Network Security Wrongful Act**.
- D. **Foreign Corrupt Practices Act:** any violation of the Foreign Corrupt Practices Act, and any amendments to such Act or any rules or regulations made under such Act, amendments to such rules and regulations, or any similar federal, state or common law.
- E. **False Claims Act:** and solely with respect to Insuring Agreement 1.5 (Privacy and Network Security Liability) and 1.6 (Media Liability), any actual or alleged violation by **You** of the False Claims Act (31 U.S.C. §§ 3729-3733), and amendments to such Act or any rules or regulations made under such Act, amendments of such Act and/or rules and regulations, or any similar federal, state, or common law anywhere in the world.

5. General Conditions

5.1 Coverage Territory

To the extent permitted by the regulations and law (which expression is for this purpose taken to include but not be limited to any trade or economic sanctions applicable to either party), and subject to the terms of this **Policy**, it covers **Wrongful Acts** committed and **Claims** made anywhere in the world.

5.2 Governing Law and Jurisdiction

This Policy is governed by and is to be interpreted in accordance with the laws of the Commonwealth of Australia and of the State or Territory of the office of the **Insurer** in which the **Policy** was issued. The courts of that State or Territory have exclusive jurisdiction in relation to any disputes regarding this **Policy** unless otherwise provided in this **Policy**.

5.3 Policy Construction

Unless the context otherwise requires, in this **Policy**:

- A. the singular includes the plural and vice versa;
- B. headings are merely descriptive and not to aid interpretation;
- C. a position, title, legal status, legal concept or structure, or statute shall include the equivalent in any other jurisdiction;
- D. a statute or statutory provision shall include any amended version or re-enactment; and
- E. capitalised words used in this **Policy** have the meanings set out in Section 3, General Definitions, and in the **Schedule**.

5.4 *Policy Limits*

- A. The **Aggregate Limits** and **Excesses** listed in the **Schedule** are separate **Aggregate Limits** and **Excesses** pertaining to each Insuring Agreement and each Insuring Agreement Extension.
- B. The total amount payable by **Us** (including **Loss**) under this **Policy** in respect of each and every **Single Claim** and in the aggregate shall not exceed the sum of the applicable **Aggregate Limits**, and is subject to the **Policy Aggregate**.
- C. The total amount payable by **Us** (including **Loss**) under this **Policy** in respect of each Insuring Agreement and each Insuring Agreement Extension shall not exceed the applicable **Aggregate Limit** or Sub-Limited **Aggregate Limit**, which is subject to the **Policy Aggregate**.
- D. Any Sub-Limit listed on the **Schedule** shall be part of and not in addition to the applicable **Aggregate Limit** shown in the **Schedule**, and subject to the **Policy Aggregate**.
- E. Sub-Limits and each Insuring Agreement Extension **Aggregate Limit** are not subject to reinstatement once exhausted.
- F. Payments of any **Loss** by **You** under **Your** applicable **Coinsurance** percentage shall not reduce the applicable Sub-Limit, **Aggregate Limit** or **Policy Aggregate**. Only the portion of any such **Loss** paid by **Us** shall reduce the applicable Sub-Limit, **Aggregate Limit** or **Policy Aggregate**. If **Coinsurance** applies to more than one Insuring Agreement, Insuring Agreement Extension or Sub-Limit thereof, the lowest applicable Sub-Limit or **Aggregate Limit** shall apply for the purposes of **Coinsurance**.
- G. If a **Neglected Software Exploit** or a **Ransomware** is covered under more than one Insuring Agreement or Insuring Agreement Extension, only the single lowest applicable Sub-Limit or **Aggregate Limit** shall apply with respect to such **Neglected Software Exploit** or **Ransomware** and the **Coinsurance** and **Excess** applicable to such limit shall also apply. If the lowest applicable Sub-Limit or **Aggregate Limit** is the same limit as another applicable Sub-Limit or **Aggregate Limit**, then the single highest applicable **Coinsurance** percentage shall apply, and the **Excess** applicable to such limit shall also apply. If the applicable Sub-Limit or **Aggregate Limit** and the **Coinsurance** percentage are the same, then the single highest applicable **Excess** shall apply.

RANSOMWARE SUB-LIMIT

Any covered **Loss** on account of any **Single Claim** in respect of a **Cyber Incident** and/or **Business Interruption Incident** and/or **Cyber Extortion Event** and/or **Privacy and Network Security Wrongful Act** arising out of a **Ransomware** is subject to the applicable **Excess** and **Coinsurance** for **Ransomware** and the Ransomware Sub-Limit, shown at Item 3 of the **Schedule**.

NEGLECTED SOFTWARE EXPLOIT SUB-LIMIT

Any covered **Loss** on account of any **Single Claim** in respect of a **Cyber Incident** and/or **Business Interruption Incident** and/or **Cyber Extortion Event** and/or **Privacy and Network Security Wrongful Act** arising out of a **Neglected Software Exploit** is subject to the applicable **Excess** and **Coinsurance** for a **Neglected Software Exploit** and the Neglected Software Exploit Sub-Limit, shown at Item 3 of the **Schedule**.

5.5 *Excess*

- A. **We** will only be liable for that part of a **Loss** and any other covered amount payable arising from any **Claim**, which exceeds the **Excess**. Such **Excess** shall be borne by **You** and is uninsured by **Us**.

- B. Only one **Excess** amount shall apply to each and every **Single Claim**.
- C. Where a **Single Claim** is subject to different **Excess** amounts, it is agreed that only the single largest applicable **Excess** shall apply.
- D. With respect to Insuring Agreement 1.2 Business Interruption, **We** will pay the **Business Interruption Loss** incurred by **You**:
 - i. once the applicable **Waiting Period** has expired; and
 - ii. which exceeds the **Excess** amount shown in Item 3 of the **Schedule**.

Business Interruption Loss does not include amounts that accrued during the **Waiting Period**.

5.6 *Related Claims and Matters*

A **Single Claim** shall attach to the **Policy** only if the notice of the first **Claim** or other matter giving rise to a **Claim** that became such **Single Claim**, was given by the **Insured** during the **Policy Period**.

5.7 *Cancellations*

You may cancel this **Policy** by giving written notice to **Us**. If there are no **Claims** notified to **Us** under this **Policy**, **We** will allow a refund of unearned premium calculated pro-rata from the time of cancellation to the natural expiry of the **Policy**.

We may cancel this **Policy** for non-payment of premium by thirty (30) days' notice given to **You** and in accordance with the requirements of any applicable legislation.

5.8 *Transactions*

In the event that a **Transaction** occurs during the **Policy Period**, then **We** will only pay for a **Loss** for any **Wrongful Act** occurring prior to the **Transaction** and which is otherwise covered by this **Policy** and reported to **Us** pursuant to General Condition 5.10 Notification.

However, the company shown in Item 1 of the **Schedule** may, up to forty-five (45) days after the **Transaction**, request an offer from **Us** for an **Extended Reporting Period** of up to eighty-four (84) months from the expiry date of the **Policy Period**. Upon such request and following **Our** receipt of any requested information, **We** shall offer to extend the cover under this **Policy** for an **Extended Reporting Period** of up to eighty-four (84) months on such terms and conditions and at such premium as **We** may decide at **Our** discretion. Any additional premium will be non-refundable.

5.9 *Acquisitions and Creations of New Subsidiaries*

The definition of **Subsidiary** under this **Policy** is extended to include any company that becomes a **Subsidiary** during the **Policy Period**, provided that:

- A. the new **Subsidiary** does not increase the **Insured Organisation's** total turnover by more than twenty percent (20%) based on the **Insured Organisation's** latest audited consolidated financial statements or annual report; and
- B. the new **Subsidiary** is domiciled outside of Canada or The United States of America or its Territories; and
- C. the new **Subsidiary** is not registered as an investment advisor with the US Securities and Exchange Commission; and
- D. the new **Subsidiary's** business activities are not materially different in their nature to those of the **Insured Organisation**.

In respect of any new **Subsidiary** falling outside the terms of conditions A.-D. above, cover will be automatically provided for a period of sixty (60) days from the date of acquisition, incorporation or creation. This automatic cover may be extended beyond the sixty (60) days with the written agreement of the **Insurer** on such terms the **Insurer** may apply and endorse to the **Policy**.

In respect of any new **Subsidiary**, cover only applies to **Claims** first made during the **Policy Period** in respect of **Wrongful Acts** allegedly committed after the acquisition or creation of the new **Subsidiary**.

5.10 *Notification*

- A. **You** shall give written notice to **Us** as soon as reasonably practicable of a **Claim**.
- B. If this **Policy** is not renewed, **You** shall give written notice to **Us** as soon as reasonably practicable of a **Claim** and in no event more than sixty (60) days after the expiry of the **Policy Period** or **Extended Reporting Period**.
- C. All notifications under this **Policy** must be provided to **Us** via the following email address: aus.financiallinesclaims@chubb.com.
- D. **You** must use **Your** best endeavors to provide all of the following information required by **Us**.
- i. Notifications under this **Policy** shall include the following information, to the best extent such information is obtainable:
 - (1) a specific description of the alleged **Claim** or **Loss** or other conduct;
 - (2) details of all parties involved, inclusive of names and contact information;
 - (3) a copy of any **Privacy and Network Security Claim** or **Media Claim** made by any third party or the documents or notice related to a **Regulatory Proceeding**;
 - (4) complete details of any alleged **Damages**; and
 - (5) such other information as **We** may reasonably require, provided that the request for information is sufficiently specific and allows a reasonable and proportionate period of time for such information to be collected.
 - ii. Requests made by **You** for indemnity by **Us** for any **Business Interruption Loss** shall be accompanied by a computation of the loss. This shall set out in detail how the loss has been calculated and what assumptions have been made. **You** shall produce any documentary evidence reasonably within **Your** power to provide, including any applicable reports, books of accounts, bills, ledgers, invoices, and other vouchers and copies of such which **We** may reasonably require.
- E. If, during the **Policy Period** or an obtained **Extended Reporting Period**, **You**:
- i. become aware of circumstances which are reasonably likely to give rise to a **Claim** and give written notice of such circumstances to **Us**; or
 - ii. receive a written request to waive application of a limitation period to, or to suspend the running of time towards expiry of a limitation period for the commencement of a civil proceeding against **You** for a **Wrongful Act** occurring before the expiry of the **Policy Period** and give written notice of such request and of such **Wrongful Act** to **Us**;
- then any **Claims** subsequently arising from such circumstances or such request shall be deemed to have first been made during the **Policy Period**.
- F. **You** shall report a **Ransomware** to the appropriate law enforcement agencies as soon as reasonably practicable.

5.11 *Calculation of Business Interruption Loss*

Our adjustment of the **Business Interruption Loss** shall take full account of trends or circumstances during the twelve (12) months immediately before the **Business interruption**

Incident, which affect the profitability of the business and would have affected the profitability of the business, whether positively or negatively, had the **Business Interruption Incident** not occurred, including all material changes in market conditions which would affect the **Net Profit** generated. However, **Our** adjustment will not include any increase in income that would likely have been earned as a result of an increase in the volume of business due to favourable business conditions.

5.12 *Valuation*

For the purposes of establishing the value of:

- A. **Direct Financial Loss** payable by **Us**, the following valuation shall apply:
- i. for currency other than that in which the **Policy** has been issued as referenced in the **Policy Schedule**, the value of that currency based on the rate of exchange published in *The Financial Times* on the day the **Theft** is first discovered by any **Control Group** member;
 - ii. **Securities** payable by **Us**, the lesser of the following shall apply:
 - a) the closing price of the **Securities** on the business day immediately preceding the day on which the **Theft** is first discovered by any **Control Group** member;
or
 - b) the cost of replacing the **Securities**; and

- B. **Cyber Extortion Damages** and/or **Reward Expenses** reimbursable by **Us**, the following valuation shall apply:

If **Cyber Extortion Damages** and/or **Reward Expenses** are paid in a currency, including cryptocurrency(ies), other than the local currency from where this **Policy** is issued or the currency in which the **Policy** is issued, then reimbursement under this **Policy** will require submission of proof of the calculation of the applicable rate of exchange used to convert such other currency to the local currency from where this **Policy** is issued or the currency in which this **Policy** is issued on the date that the **Cyber Extortion Damages** and/or **Reward Expenses** were actually paid.

Reimbursement of the **Direct Financial Loss** and/or **Cyber Extortion Damages** and/or **Reward Expenses** to **You** from **Us** under this **Policy** shall be made in the local currency from where this **Policy** is issued based on the submission of proof provided by **You**. **We** retain the right to dispute or adjust the calculation of **Direct Financial Loss** and/or **Cyber Extortion Damages** and/or **Reward Expenses** to the extent that the submission of proof **You** submit is based on an inaccurate or inflated rate of exchange. In the event that **We** dispute or adjust the valuation in accordance with this clause, **We** shall provide **You** with written reasons for doing so.

5.13 *Allocation*

In the event that any **Claim** involves both covered matters and matters not covered, a fair and proper allocation of any **Loss** shall be made between **You** and **Us** taking into account the relative legal and financial exposures attributable to covered matters and matters not covered under this **Policy**.

5.14 *Conduct of Proceedings*

- A. In respect of Insuring Agreements 1.5 and 1.6, **We** may take over and conduct (in **Your** name) the defence of any **Privacy and Network Security Claim** or **Media Claim** in respect of which **We** may be liable to indemnify **You**.
- B. **You** agree to take significant care to avoid any act or failure to act which will or might prejudice **Us** in respect of a **Privacy and Network Security Claim** or **Media Claim** covered by this **Policy**.

- C. **You** must not make any admission of liability in respect of, or agree to settle, any **Privacy and Network Security Claim** or **Media Claim**, including any **Expenses**, without **Our** prior consent (which shall not be unreasonably delayed or withheld), and **We** must be consulted in advance of investigation, defence and settlement of any **Privacy and Network Security Claim** or **Media Claim**. **You** must, at **Your** own expense, provide **Us** and any investigators or legal representatives appointed by **Us**, all information, full co-operation and assistance where reasonably required and which is reasonably within **Your** power to provide in the conduct of the investigation (including for the purpose of enabling **Us** to determine liability to provide indemnity under this **Policy**), defence, settlement, avoidance or reduction of any actual or possible **Loss** or **Claims**.

5.15 *Disputes Involving Defence & Settlement of Claims*

- A. Where a dispute arises between **You** and **Us** as to whether a **Privacy and Network Security Claim** or **Media Claim** under this **Policy** should be settled or a judgment or determination appealed, **We** will be entitled to brief senior counsel (to be mutually agreed or, in default of agreement, **You** are to select one of the three senior counsel nominated by **Us**), to advise on whether or not the **Privacy and Network Security Claim** or **Media Claim** should be contested, and if not, on the amount for which the **Privacy and Network Security Claim** or **Media Claim** should be settled or whether a judgment or determination should be appealed. In providing such advice and in making any recommendation as to settlement, senior counsel is entitled to take into account both legal and commercial considerations. Senior counsel must have regard to the damages and costs that are likely to be recovered, the defence costs that will be incurred in contesting the **Privacy and Network Security Claim** or **Media Claim** and the prospects of the **Privacy and Network Security Claim** or **Media Claim** being successfully defended. **You** will not be required to contest the **Privacy and Network Security Claim** or **Media Claim** unless senior counsel recommends that, having regard to all the circumstances, the **Privacy and Network Security Claim** or **Media Claim** should be contested.
- B. The costs of obtaining this recommendation will be treated by **Us** as part of **Expenses**.
- C. If senior counsel recommends that, having regard to all the circumstances, settlement of the **Privacy and Network Security Claim** or **Media Claim** should be attempted, then subject to receiving the **Insured's** consent (not to be unreasonably withheld or delayed), **We** will attempt settlement of the **Privacy and Network Security Claim** or **Media Claim** in accordance with senior counsel's recommendation. Where settlement is attempted in accordance with senior counsel's recommendation but is unsuccessful, **We** will continue to indemnify the **Insured** subject to the terms, conditions, exclusions and limitations of this **Policy**.
- D. In addition to the preceding provisions of this clause, where **We** have the right to conduct the defence of any **Privacy and Network Security Claim** or **Media Claim**, **We** are also entitled to settle such **Privacy and Network Security Claim** or **Media Claim** if it is in receipt of senior counsel's opinion that settlement of the **Privacy and Network Security Claim** or **Media Claim** should be attempted, having regard to the matters set out in clause A above. In such circumstances, **We** will consult with the **Insured** the subject of the **Privacy and Network Security Claim** or **Media Claim**. Should the **Insured** elect not to attempt settlement in accordance with senior counsel's recommendations and elect to contest the **Privacy and Network Security Claim** or **Media Claim**, **Our** liability will be limited to the settlement amount recommended by senior counsel, plus the **Expenses** incurred up to the date the recommendation was made. Despite any advice from such senior counsel, **We** shall be entitled, if **We** elect to do so in **Our** absolute discretion acting reasonably, to continue to defend such **Privacy and Network Security Claim** or **Media Claim**.
- E. Any election under this Condition must be made in writing to **Us** as soon as practicable, but no later than fourteen (14) days following receipt of senior counsel's recommendation.

5.16 *Non-Renewal Extended Reporting Periods*

If on expiry, any Insuring Agreement under this **Policy** is neither renewed nor replaced with insurance providing such coverage with any insurer, any **Insured** is entitled to an **Extended Reporting Period** of sixty (60) days automatically for no additional premium and may, subject to the payment of an additional payment of one hundred percent (100%) of the **Premium**, extend the cover under that Insuring Agreement of this **Policy** for an **Extended Reporting Period** of twelve (12) months from the expiration of the **Policy Period**, provided that:

- A. the extended cover under this Condition applies only to:
 - i. for Insuring Agreements 1.1, 1.2, 1.3 and 1.4, and all applicable Insuring Agreement Extensions, **Wrongful Acts** occurring before the expiry of the **Policy Period** and notified to **Us** before the expiry of the **Extended Reporting Period**; and
 - ii. for Insuring agreements 1.5 and 1.6 **Privacy and Network Security Wrongful Acts** or **Media Wrongful Acts** wholly committed before the expiry of the **Policy Period** and notified to **Us** before the expiry of the **Extended Reporting Period**.
- B. To exercise this **Extended Reporting Period** under this Condition, the **Named Insured** must, within the sixty (60) day period after the expiration of the **Policy Period**:
 - i. provide notice to **Us** of the intention to exercise the twelve (12) month option; and
 - ii. pay the additional premium.

You shall not have the right to purchase the twelve (12) month **Extended Reporting Period** under this Condition in the event that a **Transaction** occurs during the **Policy Period**.

The **Extended Reporting Period** is not available in the event this Policy is cancelled or voided. Any additional premium payable under this Condition will be fully earned upon payment and will be non-refundable.

You agree that **Our** offer of renewal terms, conditions, limits of liability or premium different from those of this **Policy** do not constitute a refusal to renew.

There shall be no entitlement to an **Extended Reporting Period** in the event, and from the date that, the **Named Insured** obtains any similar insurance cover. In such an event, any **Extended Reporting Period** already purchased shall automatically be cancelled. The premium shall have been fully earned at inception of the Extended Reporting Period.

5.17 *Subrogation*

- A. If any payment is made by **Us** under this **Policy**, **We** will be subrogated to all of **Your** rights of indemnity, contribution or recovery in relation to that payment.
- B. **You** must, at **Your** own expense, provide **Us** with all reasonable assistance and cooperation that is reasonably within **Your** power to provide in securing and enforcing such rights.
- C. **You** must not surrender any right, or settle any **Claim** for indemnity, contribution or recovery, without **Our** prior written consent, which will not be unreasonably withheld or delayed.

5.18 *Severability*

- A. The proposal submitted to **Us** for the purpose of seeking cover under this **Policy** will be construed as a separate proposal by each of **You** and, with respect to statements and particulars provided in the proposal, no statements made or information possessed by any **Insured Person** shall be imputed to any other **Insured Person** to determine whether cover is available for that **Insured**.

- B. Only the statements made or knowledge possessed by any past, present or future **Control Group** member will be imputed to such **Insured Organisation**.

5.19 *Confidentiality*

You must not disclose the terms or nature of any **Excess, Sub-Limit, Coinsurance, Aggregate Limit, Policy Aggregate** or the premium payable under this **Policy**, to any third party, including disclosure in the **Insured Organisation's** annual report, except where:

- A. **We** provide **Our** written consent, (which will not be unreasonably delayed or withheld); or
- B. it is necessary for **You** to provide, or cause to have provided, an insurance certificate to a client.
- C. disclosure is required by Court order.

5.20 *Assignment*

This **Policy** and any rights arising under this **Policy** cannot be assigned without **Our** prior written consent, which shall not be unreasonably delayed or withheld.

5.21 *Other Insurance*

- A. If any **Loss** is insured under any other policy entered into by, or effected on behalf of **You**, or under which **You** are a beneficiary, whether prior or current, then to the extent legally permissible by the Insurance Contracts Act 1984 (Cth), this **Policy**, subject to its limitations, conditions, provisions and other terms, will only cover such **Loss** to the extent that the amount of it is in excess of the amount of such other insurance.
- B. Clause A above does not apply to such other insurance that is written specifically as excess insurance over the Sub-Limit and/or **Aggregate Limit** and/or **Policy Limit** specified in the **Schedule**.

5.22 *Authorisation*

The **Named Insured** agrees to act on behalf of **You** with respect to this **Policy**.

5.23 *Trade and Economic Sanctions*

We shall not be deemed to provide cover and **We** shall not be liable to pay any **Loss** or provide any benefit under this **Policy** to the extent that the provision of such cover, payment of such **Loss** or provision of such benefit would expose **Us**, or **Our** parent or ultimate holding company, to any sanction, prohibition or restriction implemented pursuant to resolutions of the United Nations or the trade and economic sanctions, laws or regulations of the European Union, United Kingdom, Commonwealth of Australia or United States of America.

Cyber Enterprise Risk Management Version 2.2 Endorsement(s)

The following endorsement(s) varies the standard terms of **Your Policy**. It may expand, reduce, or impose additional conditions on **Your** cover as set out in the standard **Policy** terms and should be read carefully.

Privacy Statement

In this Statement “We”, “Our” and “Us” means Chubb Insurance Australia Limited (**Chubb**).

“You” and “Your” refers to Our customers and prospective customers as well as those who use Our Website.

This Statement is a summary of Our Privacy Policy and provides an overview of how We collect, disclose and handle Your Personal Information. Our Privacy Policy may change from time to time and where this occurs, the updated Privacy Policy will be posted to [Our website](#).

Chubb is committed to protecting Your privacy. Chubb collects, uses and retains Your Personal Information in accordance with the requirement of the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (**APPs**), as amended or replaced from time-to-time.

Why We collect Your Personal Information

The primary purpose for Our collection and use of Your Personal Information is to enable Us to provide insurance services to You.

Sometimes, We may use Your Personal Information for Our marketing campaigns and research, in relation to new products, services or information that may be of interest to You.

How We obtain Your Personal Information

We collect Your Personal Information (which may include sensitive information) at various points including, but not limited to, when You are applying for, changing or renewing an insurance policy with Us or when We are processing a claim. Personal Information is usually obtained directly from You, but sometimes via a third party such as an insurance intermediary or Your employer (e.g. in the case of a group insurance policy). Please refer to Our Privacy Policy for further details.

When information is provided to Us via a third party We use that information on the basis that You have consented or would reasonably expect Us to collect Your Personal Information in this way. We take reasonable steps to ensure that You have been made aware of how We handle Your Personal Information.

When do We disclose Your Personal Information?

We may disclose the information We collect to third parties, including:

- the policyholder (where the insured person is not the policyholder, i.e., group policies);
- service providers engaged by Us to carry out certain business activities on Our behalf (such as claims assessors, call centres in Australia, online marketing agency, etc);
- intermediaries and service providers engaged by You (such as current or previous brokers, travel agencies and airlines);
- government agencies (where we are required to by law);
- other entities within the Chubb group of companies such as the regional head offices of Chubb located in Singapore, UK or USA (Chubb Group of Companies); and
- third parties with whom We (or the Chubb Group of Companies) have sub-contracted to provide a specific service for Us, which may be located outside of Australia (such as in the Philippines or USA). These entities and their locations may change from time-to-time. Please contact us, if you would like a full list of the countries in which these third parties are located.

In the circumstances where We disclose Personal Information to the Chubb Group of Companies, third parties or third parties outside Australia We take steps to protect Personal Information against unauthorised disclosure, misuse or loss.

Your decision to provide Your Personal Information

In dealing with Us, You agree to Us using and disclosing Your Personal Information, which will be stored, used and disclosed by Us as set out in this Privacy Statement and Our Privacy Policy.

Access to and correction of Your Personal Information

Please contact Our customer relations team on 1800 815 675 or email CustomerService.AUNZ@chubb.com if you would like:

- a copy of Our Privacy Policy, or
- to cease to receive marketing offers from Us or persons with whom We have an association.

To request access to, update or correct your Personal Information held by Chubb, please complete this [Personal Information request form](#) and return to:

Email: CustomerService.AUNZ@chubb.com

Fax: +61 2 9335 3467

Address: GPO Box 4907 Sydney NSW 2001

How to Make a Complaint

If You have a complaint or would like more information about how We manage Your Personal Information, please review Our [Privacy Policy](#) for more details, or contact:

Privacy Officer

Chubb Insurance Australia Limited

GPO Box 4907 Sydney NSW 2001

+61 2 9335 3200

Privacy.AU@chubb.com.

General Insurance Code of Practice

We are a signatory to the General Insurance Code of Practice (**Code**). The objectives of the Code are to further raise standards of service and promote consumer confidence in the general insurance industry. Further information about the Code and your rights under it is available at codeofpractice.com.au and on request. As a signatory to the Code, we are bound to comply with its terms. As part of our obligations under Parts 9 and 10 of the Code, Chubb has a [Customers Experiencing Vulnerability & Family Violence Policy](#) (Part 9) and a [Financial Hardship Policy](#) (Part 10). The Code is monitored and enforced by the Code Governance Committee.

Complaints and Dispute Resolution Process

We understand that you could be dissatisfied with our organisation, our products and services, or the complaints handling process itself. We take all our customer's concerns seriously and have detailed below the complaints process that you can access.

Complaints and Customer Resolution Service

Contact Details

If you are dissatisfied with any aspect of your relationship with Chubb including our products or services and wish to make a complaint, please contact our Complaints and Customer Resolution Service (**CCR Service**) by post, phone, fax, or email, (as below):

Complaints and Customer Resolution Service

Chubb Insurance Australia Limited

GPO Box 4065

Sydney NSW 2001

P +61 2 9335 3200

F +61 2 9335 3411

E complaints.AU@chubb.com

Our CCR Service is committed to reviewing complaints objectively, fairly and efficiently.

Process

Please provide us with your claim or policy number (if applicable) and as much information as you can about the reason for your complaint.

Our response

We will acknowledge receipt of your complaint within one (1) business day of receiving it from you.

We will investigate your complaint and keep you informed of the progress of our investigation at least every ten (10) business days and will make a decision in relation to your complaint in writing within thirty (30) calendar days. If we are unable to make this decision within this timeframe, we will provide you with a reason for the delay and advise of your right to take your complaint to the Australian Financial Complaints Authority (AFCA) as detailed below, subject to its Rules. If your complaint falls outside the AFCA Rules, you can seek independent legal advice or access any other external dispute resolution options that may be available to you.

To the extent allowable at law, if you request copies of the information we relied on to make a decision about your complaint, we must provide it within ten (10) business days of your request. Please see the General Insurance Code of Practice 2020 (codeofpractice.com.au) or contact us for further details.

Please note that if we have resolved your complaint to your satisfaction by the end of the fifth (5th) business day after we have received it, and you have not requested that we provide you a response in writing, we are not required to provide a written response. However, this exemption does not apply to complaints regarding a declined claim, the value of a claim, or about financial hardship.

External Dispute Resolution

If you are dissatisfied with our complaint determination, or we are unable to resolve your complaint to your satisfaction within thirty (30) days, you may refer your complaint to AFCA, subject to its Rules.

AFCA is an independent external dispute resolution scheme approved by the Australian Securities and Investments Commission (ASIC). We are a member of this scheme and we agree to be bound by its determinations about a dispute. AFCA provides fair and independent financial services complaint resolution that is free to consumers.

You may contact AFCA at any time at:

Australian Financial Complaints Authority
GPO Box 3
Melbourne VIC 3001
P 1800 931 678 (free call)
F +61 3 9613 6399
E info@afca.org.au
W www.afca.org.au

Time limits may apply to complain to AFCA and so you should act promptly or otherwise consult the AFCA website to find out if or when the time limit relevant to your circumstances expires.

About Chubb in Australia

Chubb is the world's largest publicly traded property and casualty insurer. With operations in 54 countries and territories, Chubb provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. As an underwriting company, we assess, assume and manage risk with insight and discipline. We service and pay our claims fairly and promptly. The company is also defined by its extensive product and service offerings, broad distribution capabilities, exceptional financial strength and local operations globally. Parent company Chubb Limited is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index. Chubb maintains executive offices in Zurich, New York, London, Paris and other locations, and employs approximately 34,000 people worldwide.

Chubb, via acquisitions by its predecessor companies, has been present in Australia for 100 years. Its operation in Australia (Chubb Insurance Australia Limited) provides specialised and customised coverages, including Business Package, Marine, Property, Liability, Energy, Professional Indemnity, Directors & Officers, Financial Lines, Utilities, as well as Accident & Health insurance, to a broad client base, including many of the country's largest companies. Chubb also serves successful individuals with substantial assets to insure and consumers purchasing travel insurance. With five branches and more than 800 staff in Australia, it has a wealth of local expertise backed by its global reach and breadth of resources.

More information can be found at www.chubb.com/au

Contact Us

Chubb Insurance Australia Limited
ABN: 23 001 642 020 AFSL: 239687

Grosvenor Place
Level 38, 225 George Street
Sydney NSW 2000
O +61 2 9335 3200
F +61 2 9335 3411
www.chubb.com/au

Chubb. Insured.SM