



# Cyber

Private enterprise

Policy document

United States

SPECIMEN

## PREAMBLE

**IMPORTANT: COVERAGE TRIGGERS.** It is important for **you** to review this Policy in its entirety carefully, including **CONDITION 1**, as the trigger for coverage, including when **you** must notify **us** of a claim, under each Section and Insuring Clause may differ.

**INSURING CLAUSES 5** and **6** provide cover on a claims made basis. **You** are provided with an automatic extended reporting period in accordance with **CONDITION 5** and entitled to purchase an optional extended reporting period in accordance with **CONDITION 6**. If **you** have any questions regarding claims made coverage or the importance of purchasing an extended reporting period, **you** are advised to contact **your** broker.

This Policy is a contract of insurance between **you** and **us**. **Your** Policy contains all the details of the cover that **we** provide. This Policy consists of and must be read together with the Declarations page and any Endorsements. This Policy is not complete unless it is signed and a Declarations page is attached.

The sections of this Policy are identified by the blue lines across the page with white upper case print, these are for information purposes only and do not form part of the cover given by this Policy. Terms in bold upper case print are references to specific Insuring Clauses, Sections or Conditions. Other terms in bold lower case print are defined terms and have a special meaning as set forth in the Definitions section and elsewhere. Words stated in the singular will include the plural and vice versa.

In consideration of the **premium** and in reliance upon the information that **you** have provided to **us** prior to the commencement of this insurance, **we** agree to provide the cover as set out below:

## INSURING CLAUSES

### INSURING CLAUSE 1: CYBER INCIDENT RESPONSE

#### SECTION A: INCIDENT RESPONSE COSTS

**We** agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. gain access to **our 24/7 cyber incident response line**;
- b. engage with **our cyber incident manager** who will coordinate the initial response;
- c. obtain initial advice and consultancy from **our cyber incident manager**, including threat intelligence in relation to the **cyber event**; and
- d. obtain initial remote support and assistance from **our cyber incident manager** to respond to the **cyber event**.

## SECTION B: LEGAL AND REGULATORY COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. obtain initial legal advice to determine **your privacy breach** notification obligations;
- b. draft notification letters, substitute notices, website notices or e-mail notification templates; and
- c. notify any appropriate government, regulatory, law enforcement, professional or statutory body.

## SECTION C: IT SECURITY AND FORENSIC COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. engage with an external IT security consultant to identify the source and scope of the **cyber event**;
- b. obtain initial advice to remediate the impact of the **cyber event**;
- c. conduct a forensic investigation of **your computer systems** where reasonable and necessary or as required by law or a regulatory body (including a requirement for a PCI Forensic Investigator);
- d. contain and remove any malware discovered on **your computer systems**; and
- e. engage with an IT security consultant to provide expert witness testimony at any trial or hearing arising from the **cyber event**.

## SECTION D: CRISIS COMMUNICATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. engage with a crisis communications consultant to obtain specific advice in direct relation to the **cyber event**;
- b. coordinate media relations in response to the **cyber event**;
- c. receive training for relevant spokespeople with respect to media communications in direct relation to the **cyber event**; and
- d. formulate a crisis communications plan in order to reduce damage to **your** brand and reputation as a direct result of the **cyber event**.

## SECTION E: PRIVACY BREACH MANAGEMENT COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, as a direct result of a **cyber event** first discovered during the **period of the policy** to:

- a. print and post appropriate notices for any individual affected by the actual or suspected **cyber event** or to send e-mail notices or issue substitute notices;
- b. provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;

- c. set up a call center to manage inbound and outbound calls in direct relation to the **cyber event**; and
- d. provide translation services to manage communications with affected individuals.

#### SECTION F: THIRD PARTY PRIVACY BREACH MANAGEMENT COSTS

We agree to pay on behalf of any **third party** any reasonable sums necessarily incurred as a direct result of a **cyber event** first discovered by **you** during the **period of the policy** to:

- a. print and post appropriate notices for any individual affected by the actual or suspected **cyber event** or to send e-mail notices or issue substitute notices;
- b. provide credit monitoring services, identity monitoring services, identity restoration services or identity theft insurance to affected individuals;
- c. set up a call center to manage inbound and outbound calls in direct relation to the **cyber event**; and
- d. provide translation services to manage communications with affected individuals;

provided that **you** have contractually indemnified the **third party** against this **cyber event** and they have a legal obligation to notify affected individuals and that any costs incurred are with a provider that **we** have selected and approved in conjunction with **you**.

#### SECTION G: POST BREACH REMEDIATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred by **you**, or on **your** behalf, with **our cyber incident manager** for any services that will mitigate the potential of a future **cyber event** following a **cyber event** covered under **INSURING CLAUSE 1 (SECTIONS A, B, C, D, E and F only)**.

#### INSURING CLAUSE 2: CYBER CRIME

##### SECTION A: ELECTRONIC THEFT OF YOUR FINANCIAL ASSETS

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of any **third party** committing an unauthorized electronic transfer of **your** financial assets from a bank or other financial institution, including an asset management firm, pension or investment fund.

##### SECTION B: ELECTRONIC THEFT OF THIRD PARTY FUNDS HELD IN ESCROW

We agree to reimburse **you** for **loss** (including compensation **you** are legally obliged to pay) first discovered by **you** during the **period of the policy** as a direct result of **you** having to reimburse any **third party** for theft from a bank account held in **your** name of money or other financial assets held by **you** on behalf of that **third party**, provided that the theft was committed by electronic means by any other **third party**.

##### SECTION C: ELECTRONIC THEFT OF PERSONAL FINANCIAL ASSETS

We agree to reimburse any **senior executive officer** for personal financial loss first discovered by them during the **period of the policy** as a direct result of any **third party** compromising the **company's** network security which results in:

- a. theft of money or other financial assets from a personal bank account of the **senior executive officer**; or
- b. identity theft of the **senior executive officer** as a result of a **privacy breach** suffered by **you**.

#### SECTION D: EXTORTION

We agree to reimburse **you** for any ransom paid by **you**, or on **your** behalf, in response to an extortion demand first discovered by **you** during the **period of the policy** as a direct result of any threat to:

- a. introduce malware, or the actual introduction of malware, including Ransomware, into **your computer systems**;
- b. prevent access to **your computer systems** or data or any **third party** systems hosting **your** applications or data;
- c. reveal **your** confidential information or confidential information entrusted to **you**; or
- d. damage **your** brand or reputation by posting false or misleading statements about **you** on social media sites.

#### SECTION E: AUTHORIZED PUSH PAYMENT FRAUD

We agree to reimburse **you** for **loss** first discovered by **you** during the **period of the policy** as a direct result of any phishing, vishing or other social engineering attack against any **employee** that results in the electronic transfer of:

- a. **your** funds; or
- b. **third party** funds from a bank account held by **you** on behalf of the **third party**;

authorized by **you**, to an unintended **third party**, including fake invoice scams and CEO fraud.

#### SECTION F: TELEPHONE HACKING

We agree to reimburse **you** for **loss** associated with the cost of unauthorized calls or unauthorized use of **your** bandwidth first discovered by **you** during the **period of the policy** as a direct result of **your** telephone system being hacked by a **third party**.

#### SECTION G: UNAUTHORIZED USE OF COMPUTER RESOURCES

We agree to reimburse **you** for **loss** associated with increased electricity costs and cloud service billing first discovered by **you** during the **period of the policy** as a direct result of **cryptojacking** or **botnetting**.

### INSURING CLAUSE 3: SYSTEM DAMAGE AND BUSINESS INTERRUPTION

#### SECTION A: SYSTEM DAMAGE AND RECTIFICATION COSTS

We agree to reimburse **you** for the reasonable and necessary additional costs of employing specialist data recovery consultants, including IT forensic consultants, to recover **your** data or applications as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**.



## SECTION B: INCOME LOSS AND EXTRA EXPENSE

We agree to reimburse **you** for **your income loss** and **extra expense** sustained during the **indemnity period** as a direct result of an interruption to **your** business activities arising directly out of any sudden, unexpected and continuous outage of **your computer systems** which is first discovered by **you** during the **period of the policy**, provided that the **computer systems** outage lasts longer than the **waiting period** and arises directly out of any **cyber event**.

## SECTION C: DEPENDENT BUSINESS INTERRUPTION

We agree to reimburse **you** for **your income loss** and **extra expense** sustained during the **indemnity period** as a direct result of an interruption to **your** business activities arising directly out of any sudden, unexpected and continuous outage of computer systems used directly by a **supply chain partner** which is first discovered by **you** during the **period of the policy**, provided that the computer systems outage lasts longer than the **waiting period** and arises directly out of any **cyber event**.

## SECTION D: CLAIM PREPARATION COSTS

We agree to pay on **your** behalf any reasonable sums necessarily incurred for professional fees to determine the amount of **your income loss** and **extra expense** sustained following an event covered under **INSURING CLAUSE 3 (SECTIONS B and C only)**.

## INSURING CLAUSE 4: NETWORK SECURITY & PRIVACY LIABILITY

### SECTION A: NETWORK SECURITY LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) as a result of any **claim** arising directly out of a **cyber event** first discovered by **you** during the **period of the policy** that results in:

- a. the transmission of malware to a **third party's** computer system;
- b. **your computer systems** being used to carry out a denial of service attack;
- c. **your** failure to prevent unauthorized access to information stored or applications hosted on **your computer systems**; and
- d. identity theft, experienced by **your employees** or any **third party**.

We will also pay **costs and expenses** on **your** behalf.

### SECTION B: PRIVACY LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including the establishment of any consumer redress fund and associated expenses) as a result of any **claim** arising directly out of a **cyber event** first discovered by **you** during the **period of the policy** that results in:

- a. an actual or suspected disclosure of or unauthorized access to any Personally Identifiable Information (PII), including payment card information or Protected Health Information (PHI);

- b. **your** failure to adequately warn affected individuals of a **privacy breach**, including the failure to provide a data breach notification in a timely manner;
- c. a breach of any rights of confidentiality as a direct result of **your** failure to maintain the confidentiality of any data pertaining to an **employee**;
- d. a breach of any rights of confidentiality, including a breach of any provisions of a non-disclosure agreement or breach of a contractual warranty relating to the confidentiality of commercial information, PII, or PHI;
- e. a breach of any part of **your** privacy policy; or
- f. actual or suspected disclosure of or unauthorized access to **your** data or data for which **you** are responsible.

We will also pay **costs and expenses** on **your** behalf.

#### SECTION C: MANAGEMENT LIABILITY

We agree to pay on behalf of any **senior executive officer** all sums they become legally obliged to pay as a result of any **claim** made against them arising directly out of a **cyber event** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on behalf of **your** senior executive officers.

However, **we** will not make any payment under this Section for which the **senior executive officer** is entitled to indemnity under any other insurance, except for any additional sum which is payable over and above the other insurance.

#### SECTION D: REGULATORY INVESTIGATION COSTS

We agree to pay on **your** behalf any fines and penalties resulting from a **regulatory investigation** arising as a direct result of a **cyber event** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

#### SECTION E: MERCHANT SERVICES LIABILITY

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay **your** acquiring bank or payment processor, including card brand assessments, fraud recoveries, operational reimbursements, non-cooperation costs and case management fees as a direct result of a **payment card breach** first discovered by **you** during the **period of the policy**.

We will also pay **costs and expenses** on **your** behalf.

#### INSURING CLAUSE 5: MEDIA LIABILITY

##### SECTION A: DEFAMATION

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** or any applicable extended reporting period for any:

- a. defamation, including but not limited to libel, slander, trade libel, product disparagement and injurious falsehood; or
- b. emotional distress or outrage based on harm to the character or reputation of any person or entity;

arising out of any **media content**.

We will also pay **costs and expenses** on **your** behalf.

#### SECTION B: INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' costs and expenses) as a result of any **claim** first made against **you** during the **period of the policy** or any applicable extended reporting period for any:

- a. infringement of any intellectual property rights, including but not limited to, copyright, trademark, trade dilution, trade dress, commercial rights, design rights, domain name rights, image rights, moral rights, service mark or service name, but not including patent;
- b. act of passing-off, piracy or plagiarism or any misappropriation of content, concepts, format rights or ideas or breach of a contractual warranty relating to intellectual property rights;
- c. breach of any intellectual property rights license acquired by **you**; or
- d. failure to attribute authorship or provide credit;

arising out of any **media content**.

We will also pay **costs and expenses** on **your** behalf.

#### INSURING CLAUSE 6: TECHNOLOGY ERRORS AND OMISSIONS

We agree to pay on **your** behalf all sums which **you** become legally obliged to pay (including liability for claimants' **costs and expenses**) as a result of any **claim** first made against **you** during the **period of the policy** or any applicable extended reporting period arising out of any act, error, omission or breach of contract in the provision of **your technology services**.

We will also pay **costs and expenses** on **your** behalf.

### HOW MUCH WE WILL PAY

The maximum amount payable by **us** under this Policy in total across all Insuring Clauses will not exceed the **policy limit**.

The maximum amount payable by **us** in respect of each Section and each Insuring Clause will not exceed the **insured limit** for that Section or Insuring Clause.



Where cover is provided under multiple Sections of one or more Insuring Clauses, the maximum amount **we** will pay in total for that claim is the amount of the highest **insured limit** of the Sections under which cover is provided.

Where more than one claim under this Policy arises from the same original cause or single source or event, all of those claims will be deemed to be one claim and only one **insured limit** will be applicable.

## YOUR DEDUCTIBLE

**We** will only be liable for that part of each and every claim which exceeds the amount of the **deductible**. If any expenditure is incurred by **us** which falls within the amount of the **deductible**, then **you** will reimburse that amount to **us** upon **our** request.

Where more than one claim arises from the same original cause or single source or event all of those claims will be deemed to be one claim and only one **deductible** will apply.

In respect of **INSURING CLAUSE 3 (SECTIONS B and C only)**, a single **waiting period, deductible** and **indemnity period** will apply to each claim. Where the same original cause or single source or event causes multiple computer system outages, these will be considered one computer system outage whose total duration is equal to the cumulative duration of each individual outage.

Where cover is provided under multiple Sections or multiple Insuring Clauses only one **deductible** will apply to that claim and this will be the highest **deductible** of the Sections under which cover is provided.

## DEFINITIONS

1. **"Approved claims panel providers"** means  
the approved claims panel providers stated in the Declarations page.
2. **"Botnetting"** means  
the unauthorized use of **your computer systems** by a **third party** for the purpose of launching a denial of service attack or hacking attack against another **third party**.
3. **"Claim"** means
  - a. a written demand for compensation;
  - b. a written request for a retraction or a correction;
  - c. a threat or initiation of a lawsuit; or
  - d. a disciplinary action or **regulatory investigation**;made against **you**.

4. "Client" means

any **third party** with whom **you** have a contract in place for the supply of **your** business services in return for a fee, or where a fee would normally be expected to be paid.

5. "Company" means

the company named as the Insured in the Declarations page or any **subsidiary**.

6. "Computer systems" means

all electronic computers used directly by **you**, including operating systems, software, hardware and all communication and open system networks and any data or websites wheresoever hosted, off-line media libraries and data back-ups and mobile devices including but not limited to smartphones, iPhones, tablets or personal digital assistants.

7. "Continuity date" means

the **effective date** or if **you** have maintained uninterrupted insurance of the same type with **us**, the date this insurance was first incepted with **us**.

8. "Costs and expenses" means

- a. **third party** legal and professional expenses (including disbursements) reasonably incurred in the defense of **claims**, or the circumstances which could reasonably be expected to give rise to a **claim** or in quashing or challenging the scope of any injunction, subpoena or witness summons;
- b. any post judgment interest;
- c. the cost of appeal, attachment and similar bonds including bail and penal bonds; and
- d. **your** reasonable costs of attend court or any tribunal, arbitration, adjudication, mediation or other hearing in connection with any **claim**.

Subject to all **costs and expenses** being incurred with the **cyber incident manager's** prior written agreement.

9. "Cryptojacking" means

the unauthorized use of **your computer systems** by a **third party** for the sole purpose of cryptocurrency mining activities.

10. "Cyber event" means

any actual or suspected unauthorized access to, or electronic attack on, **your computer systems**, or in respect of **INSURING CLAUSE 3 (SECTION C)** only computer systems used directly by a **supply chain partner**, including a denial of service attack, cyber terrorism, hacking attack, Trojan horse, phishing attack, man-in-the-middle attack, application-layer attack, compromised key attack, malware infection (including spyware or Ransomware) or computer virus.

"Cyber event" also means any **privacy breach**.

11. "**Cyber incident manager**" means  
the company or individual named as the cyber incident manager in the Declarations page.
12. "**Cyber incident response line**" means  
the telephone number stated as the cyber incident response line in the Declarations page.
13. "**Deductible**" means  
the amount stated as the deductible in the Declarations page.
14. "**Effective date**" means  
the effective date stated in the Declarations page.
15. "**Employee**" means  
any employee of the **company**, any volunteer working for the **company** and any individual working for the **company** as an independent contractor.
16. "**Expiration date**" means  
the expiration date stated in the Declarations page or the date the Policy is cancelled in accordance with **CONDITION 4** or terminated in accordance with **CONDITION 8**.
17. "**Extra expense**" means  
**your** reasonable sums necessarily incurred in addition to **your** normal operating expenses to mitigate an interruption to and continue **your** business activities, provided that the costs are less than **your** expected **income loss** sustained during the **indemnity period** had these measures not been taken.
18. "**Funds transfer policy**" means  
a **company** policy that requires an **employee** to verify the authenticity or validity of any instruction or communication requesting a:
- transfer of funds above USD10,000 prior to the transfer being made; or
  - change to **client** account details prior to any transfer of funds being made to this **client** or account by **you**;
- using contact information that was not acquired from the same instruction or communication and by a method that is different to the method the instruction or communication is received by.
19. "**Income loss**" means  
**your** income that, had the **cyber event** which gave rise to the claim not occurred, would have been generated directly from **your** business activities (less sales tax) during the **indemnity period**, less:
- actual income (less sales tax) generated directly from **your** business activities during the **indemnity period**; and

b. any cost savings achieved as a direct result of the reduction in income.

20. **"Indemnity period"** means

the period starting from the first occurrence of:

- a. the **computer systems** outage; or
- b. the outage of computer systems used directly by a **supply chain partner**;

and lasting for the period stated as the indemnity period in the Declarations page.

21. **"Insured limit"** means

the aggregate limit of liability stated in the Declarations page, which is the maximum amount payable by **us** in respect of all claims under this Policy for that Section or Insuring Clause.

22. **"Loss"** means

any direct financial loss sustained by the **company**.

23. **"Media content"** means

any content created or disseminated by **you** or on **your** behalf, distributed through online digital channels, including but not limited to social media, websites and mobile applications.

**"Media content"** does not include any:

- a. tangible product design;
- b. industrial design;
- c. architectural or building services;
- d. any advertisement created by **you** for a **third party**;
- e. business, company, product or trading name;
- f. product packaging or labeling; or
- g. software products.

24. **"Payment card breach"** means

an actual or suspected unauthorized disclosure of payment card data stored or processed by **you** arising out of an electronic attack, accidental disclosure or the deliberate actions of a rogue **employee**.

**"Payment card breach"** does not mean a situation where payment card data is deliberately shared with or sold to a **third party** with the knowledge and consent of a **senior executive officer**.

25. **"Period of the policy"** means

the period between the **effective date** and the **expiration date**.

26. **"Policy limit"** means

the aggregate limit of liability for all Insuring Clauses combined stated in the Declarations page.

27. **"Premium"** means  
the amount stated as the premium in the Declarations page and any subsequent adjustments.
28. **"Privacy breach"** means  
an actual or suspected unauthorized disclosure of information belonging to **you** or in **your** care, custody and control arising out of an electronic attack, accidental disclosure, theft or the deliberate actions of a rogue **employee** or **third party**.
- "Privacy breach"** does not mean a situation where information is deliberately shared with or sold to a **third party** with the knowledge and consent of a **senior executive officer**.
29. **"Regulatory investigation"** means  
a formal hearing, official investigation, examination, inquiry, legal action or any other similar proceeding initiated by a government, regulatory, law enforcement, professional or statutory body against **you**.
30. **"Senior executive officer"** means  
board members, C-level executives, in-house lawyers and risk managers of the **company**.
31. **"Subsidiary"** means  
any entity which the **company** has majority ownership of, meaning more than 50% ownership, on or before the **effective date**.
32. **"Supply chain partner"** means  
any:  
  - a. **third party** that provides **you** with hosted computing services including infrastructure, platform, file storage and application level services; or
  - b. **third party** listed as a supply chain partner in an endorsement attaching to this policy which **we** have included.
33. **"Technology services"** means  
the supply by **you** of technology services to **your client**, including but not limited to hardware, software, data processing, internet services, data and application hosting, computer systems analysis, consulting, training, programming, installation, integration, support and network management.
34. **"Third party"** means  
any person who is not an **employee** or any legal entity that is not the **company**.
35. **"Waiting period"** means  
the number of hours stated as the waiting period in the Declarations page.

36. "We/our/us" means

the insurer stated in the Declarations page.

37. "You/your" means

the **company** and **employees** solely acting in the normal course of the **company's** business activities.

## EXCLUSIONS

We will not make any payment under this Policy:

### EXCLUSIONS RELATING TO SYSTEM DAMAGE AND BUSINESS INTERRUPTION

In respect of **INSURING CLAUSE 3** only:

#### 1. Business interruption liability

for that part of any **claim** that constitutes actual or alleged liability to a **third party**, or legal costs in the defense of any **claim**, including customer compensation.

### EXCLUSIONS RELATING TO TECHNOLOGY ERRORS AND OMISSIONS

In respect of **INSURING CLAUSE 6** only:

#### 2. Product IP infringement

arising directly or indirectly from the actual or alleged theft or misappropriation of any trade secret by an **employee** from a former employer of theirs or infringement of any intellectual property right by any product manufactured, designed, formulated, licensed, distributed, or sold by **you** or the misappropriation of any trade secret by **you** or a **third party**.

### EXCLUSIONS RELATING TO ALL INSURING CLAUSES

#### 3. Antitrust

in respect of **INSURING CLAUSES 5** and **6**, for or arising out of any actual or alleged antitrust violation, restraint of trade, unfair competition, false, deceptive or unfair trade practices, violation of consumer protection laws or false or deceptive advertising.

#### 4. Associated companies

- a. in respect of any **claim** made by any company, firm or partnership in which the **company** has greater than a 10% executive or financial interest, unless the **claim** emanates from an independent **third party**;
- b. in respect of any **claim** made by any company, firm, partnership or individual which has greater than a 10% executive or financial interest in the **company**, unless the **claim** emanates from an independent **third party**;
- c. arising out of or resulting from any of **your** activities as a trustee, partner, officer, director or employee of any employee trust, charitable organization, corporation, company or business other than that of the **company**; or

d. in respect of any **claim** made by or on behalf of the **company** against a **third party**.

5. **Betterment**

which results in **you** being in a better financial position or **you** benefitting from upgraded versions of **your computer systems** over and above the position **you** were in directly before the event which gave rise to the claim under this policy, including recurring annual costs extending beyond the **period of the policy**.

However, this **EXCLUSION** will not apply to **INSURING CLAUSE 1 (SECTION G only)**.

6. **Bodily injury and property damage**

arising directly or indirectly out of bodily injury, or tangible property damage.

However, this Exclusion will not apply to **INSURING CLAUSES 4 (SECTIONS A, B and C only)** and **5** for any **claim** as a direct result of mental injury or emotional distress.

7. **Chargebacks**

for any credit card company or bank, wholly or partially reversing or preventing a payment transaction, unless specifically covered under **INSURING CLAUSE 4 (SECTION E only)** for which **you** have purchased coverage.

8. **Core internet infrastructure failure**

arising directly from a failure, material degradation or termination of any core element of the internet, telecommunications or GPS infrastructure that results in a regional, countrywide or global outage of the internet or telecommunications network, including a failure of the core DNS root servers, satellite network or the IP addressing system or an individual state or non-state actor disabling all or part of the internet.

9. **Criminal, malicious or dishonest acts of senior executive officers**

arising directly or indirectly out of any criminal, malicious or dishonest act, error or omission by a **senior executive officer**.

10. **Cryptocurrency**

arising directly or indirectly out of the theft or loss of any crypto asset, including cryptocurrency, utility tokens, securities tokens, ecosystem tokens or any other type of digital currency.

11. **Insolvency**

arising out of or relating directly or indirectly to **your** insolvency or bankruptcy, or the insolvency or bankruptcy of any **third party**. However, **your** insolvency will not relieve **us** of any of **our** legal obligations under this contract of insurance.

12. **Known claims and circumstances**

arising out of any actual or suspected **cyber event, claim** or circumstance which might give rise to a claim under this Policy of which a **senior executive officer** was aware of, or ought

reasonably to have been aware of, prior to the **continuity date**, including any claim or circumstance notified to any other insurer.

13. **Liquidated damages, service credits and penalty clauses**

for liquidated damages or service credits, or arising out of penalty clauses unless **you** would have been liable in the absence of any contract stipulating the liquidated damages or service credits or penalty clauses.

14. **Loss of economic value**

for the reduction in economic or market value (including loss of potential future sales) of any of **your** intellectual property assets.

15. **Management liability**

for any sums that **your senior executive officers** become legally obliged to pay, including **costs and expenses**, as a result of any **claim** made against them arising out of a **cyber event**.

However, this Exclusion will not apply to **INSURING CLAUSE 4 (SECTION C only)**.

16. **Merchant services costs and expenses liability**

for any sums **you** become legally obliged to pay your acquiring bank or payment processor as a direct result of a **payment card breach**.

However, this Exclusion will not apply to **INSURING CLAUSE 4 (SECTION E only)**.

17. **Misleading advertising**

arising directly or indirectly from any advertisement, promotion or product description that is actually or alleged to be false or misleading.

18. **Nuclear**

arising directly or indirectly from or contributed to by:

- a. ionizing radiations or contamination by radioactivity from any nuclear fuel or from any nuclear waste from the combustion of nuclear fuel; or
- b. the radioactive, toxic, explosive or other hazardous properties of any explosive nuclear assembly or nuclear component.

19. **Other insurance**

for which **you** are entitled to indemnity under any other insurance except for:

- a. any additional sum which is payable in excess of the other insurance where that insurance has been declared to **us**; or
- b. any contribution that **we** are obliged to make by law and that contribution will be in proportion to the indemnity available under the Policies.



20. **Patent infringement**

arising directly or indirectly out of the actual or alleged infringement of any patent or inducing the infringement of any patent.

21. **Pollution**

arising directly or indirectly out of the discharge, dispersal, release, migration, seepage or escape of any solid, liquid, gaseous, radiological or thermal irritant, toxic or hazardous substance, or contaminant, including smoke vapor, soot, fumes, acids, alkalis, chemicals and waste materials, including recycled, reconditioned or reclaimed materials.

22. **Power and utility failure**

arising directly or indirectly from any:

- a. failure in the power supply, including that caused by any surge or spike in voltage, electrical current or transferred energy; or
- b. failure, disruption or reduction in the supply of utilities, including telecommunications, gas and water infrastructure or services.

23. **Professional liability**

arising directly out of any negligent advice or professional services provided to a **client** for a fee except when arising directly from a **cyber event**.

However, this Exclusion will not apply to **INSURING CLAUSE 6**.

24. **Property and hardware costs**

for any tangible property repair or replacement including the cost of repairing any hardware or replacing any tangible property or equipment that forms part of **your computer systems**.

25. **Property perils**

arising directly or indirectly from fire, theft, earthquake or earth movement of any kind, flood, hail, hurricane, lightning strike, solar storm, tornado, tsunami, volcano, wildfire or wind.

26. **Regular hours staff costs**

for contracted salary and bonus costs paid to **employees**.

27. **Sanctions**

or will be deemed to provide any cover, to the extent that the provision of such payment or cover will expose **us** to any sanction, prohibition or restriction under the United Nations resolutions or the trade or economic sanctions, laws or regulations of Australia, Canada, the European Union, United Kingdom or United States of America.

28. **Theft of funds held in escrow**

for theft of money or other financial assets belonging to a **third party** from a bank account held by **you** on their behalf.

However, this Exclusion will not apply to **INSURING CLAUSE 2 (SECTIONS B or E only)**.

**29. Uninsurable fines**

for fines, penalties, civil or criminal sanctions or multiple, punitive or exemplary damages, unless insurable by law.

**30. Unlawful collection of data**

arising directly or indirectly out of any actual or alleged unlawful or unauthorized collection or sale of data by **you** or on **your** behalf, including but not limited to the storage of, harvesting of or processing of any such data.

**31. Unlawful surveillance**

in respect of any actual or alleged eavesdropping, wiretapping, or unauthorized audio or video recording committed by **you** or by a **third party** on **your** behalf with the knowledge and consent of **your senior executive officers**.

**32. Unsolicited communications**

arising directly or indirectly from any actual or alleged violation of:

- a. the CAN-SPAM Act of 2003 or any subsequent amendments to that Act;
- b. the Telephone Consumer Protection Act (TCPA) of 1991 or any subsequent amendments to that Act; or
- c. any other law, regulation or statute relating to unsolicited communication, distribution, sending or transmitting of any communication via telephone or any other electronic or telecommunications device.

However, this Exclusion will not apply to **INSURING CLAUSE 4 (SECTION A only)**.

**33. War**

arising directly or indirectly out of:

- a. war, including undeclared or civil war;
- b. warlike action by a military force, including action in hindering or defending against an actual or expected attack by any government, sovereign or other authority using military personnel or other agents; or
- c. insurrection, rebellion, usurped power, or action taken by governmental authority in hindering or defending against any of these.

## CONDITIONS

**1. What you must do if an incident takes place**

If any **senior executive officer** becomes aware of any incident which may reasonably be expected to give rise to a claim under this Policy, **you** must:

- a. notify the **cyber incident manager** as soon as is reasonably practicable and follow their directions. However, this notification must be made no later than 60 days following the **expiration date** or the end of any applicable extended reporting period. A telephone call to **our cyber incident response line** or confirmed notification via **our** cyber incident response app will constitute notification to the **cyber incident manager**;
- b. in respect of **INSURING CLAUSE 2**, report the incident to the appropriate law enforcement authorities; and
- c. in respect of **INSURING CLAUSES 4, 5 and 6**, not admit liability for or settle or make or promise any payment or incur any **costs and expenses** without **our** prior written agreement (which will not be unreasonably withheld).

Due to the nature of the coverage offered by this Policy, any unreasonable delay by **you** in notifying the **cyber incident manager** could lead to the size of the claim increasing or to **our** rights of recovery being restricted. **We** will not be liable for that portion of any claim that is due to any unreasonable delay in **you** notifying the **cyber incident manager** of any incident in accordance with this clause. However, if **you** are prevented from notifying **us** by a legal or regulatory obligation then **your** rights under this Policy will not be affected.

If **you** discover a **cyber event** **you** may only incur costs without **our** prior written consent within the first 72 hours following the discovery and only **third party** costs incurred must be with a company forming part of the **approved claims panel providers**. All other costs may only be incurred with the prior written consent of the **cyber incident manager** (which will not be unreasonably withheld).

**We** require **you** to provide full details of the incident, including but not limited to:

- a. the time, place and nature of the incident;
- b. the manner in which **you** first became aware of this incident;
- c. the reasons why **you** believe that this incident could give rise to a claim under this Policy;
- d. the identity of the potential claimant; and
- e. an indication as to the size of the claim that could result from this incident.

In respect of **INSURING CLAUSES 5 and 6**, if **you** notify an incident that **we** agree is reasonably expected to give rise to a **claim**, **we** will accept any **claim** that arises out of the incident as being notified under this Policy.

## 2. Agreement to pay claims (duty to defend)

**We** have the right and duty to take control of and conduct in **your** name the investigation, settlement or defense of any **claim**. **We** will not have any duty to pay **costs and expenses** for any part of a **claim** that is not covered by this Policy.

**You** may ask the **cyber incident manager** to consider appointing **your** own lawyer to defend the **claim** on **your** behalf and the **cyber incident manager** may grant **your** request if they

consider **your** lawyer is suitably qualified by experience, taking into account the subject matter of the **claim**, and the cost to provide a defense.

**We** will endeavor to settle any **claim** through negotiation, mediation or some other form of alternative dispute resolution and will pay on **your** behalf the amount **we** agree with the claimant. If **we** cannot settle using these means, **we** will pay the amount which **you** are found liable to pay either in court or through arbitration proceedings, subject to the **insured limit**.

**We** will not settle any **claim** without **your** consent. If **you** refuse to provide **your** consent to a settlement recommended by **us** and elect to continue legal proceedings in connection with the **claim**, any further **costs and expenses** incurred will be paid by **you** and **us** on a proportional basis, with 80% payable by **us** and 20% payable by **you**. As a consequence of **your** refusal, **our** liability for the **claim**, excluding **costs and expenses**, will not be more than the amount for which the **claim** could have been settled.

### 3. Calculation of business interruption losses

Following an interruption to **your** business activities covered under **INSURING CLAUSE 3**, **you** must provide **us** with **your** calculation of the loss including:

- a. how the loss has been calculated and what assumptions have been made; and
- b. supporting documents including account statements, sales projections and invoices.

### 4. Cancellation

This Policy may be cancelled by **you** by giving **us** advance written notice stating the **effective date** of the cancellation. If **you** give **us** notice of cancellation, the return **premium** will be in proportion to the number of days that the Policy is in effect.

**We** reserve the right of cancellation in the event that any amount due to **us** by **you** remains unpaid more than 60 days beyond the **effective date**. If **we** exercise this right of cancellation, **we** will send **you** written notice to **your** last mailing address shown in the Policy. **We** will also send written notice to **your** authorized insurance agent or broker.

The written notice will include the specific reason for cancellation, amount of premium due, and date the Policy will terminate. The cancellation will take effect from 15 days after the date the written notice of cancellation is issued.

### 5. Extended reporting period

In respect of **INSURING CLAUSES 5 and 6** only, an extended reporting period of 60 days (90 days if **you** are a public entity) following the **expiration date** will be automatically granted at no additional premium.

This extended reporting period will cover, subject to all other terms, conditions and exclusions of this Policy, any **claim** first made against **you** during this extended reporting period, provided that the **claim** arises out of any act, error or omission committed prior to the **expiration date**.

If any similar insurance is in force during this extended reporting period, coverage provided by this extended reporting period will be excess over the other insurance. The applicable **insured limit** and **policy limit** available to **you** during this extended reporting period will be equal to the amount of coverage remaining in the applicable **insured limit** and **policy limit** of the expiring Policy.

#### 6. Optional extended reporting period

In respect of **INSURING CLAUSES 5** and **6** only, if **we** or **you** decline to renew or cancel this Policy then **you** will have the right to be issued with an endorsement providing an optional extended reporting period for the duration stated in the Declarations page which will be effective from the termination of the automatic extended reporting period.

This optional extended reporting period will cover, subject to all other terms, conditions and exclusions of this Policy any **claim** first made against **you** and reported to **us** during this optional extended reporting period, provided that the **claim** arises out of any act, error or omission committed prior to the date of cancellation or non-renewal.

If **you** would like to purchase the optional extended reporting period, **you** must notify **us** and pay **us** the optional extended reporting period premium stated in the Declarations page within 60 days of cancellation or non-renewal.

The right to the optional extended reporting period will not be available to **you** where cancellation or non-renewal by **us** is due to non-payment of the **premium** or **your** failure to pay any amounts in excess of the applicable **insured limit** or within the amount of the applicable **deductible** as is required by this Policy in the payment of claims.

At the renewal of this Policy, our quotation of different **premium**, **deductible**, limits of liability or changes in policy language will not constitute non-renewal by **us**.

#### 7. Fraudulent claim

If it is determined by final adjudication, arbitral tribunal or written admission by **you**, that **you** notified **us** of any claim knowing it to be false or fraudulent, **we** will have no responsibility to pay that claim and **we** may recover from **you** any sums paid in respect of that claim. However, this will not affect any non-fraudulent claim under this Policy which has been previously notified to **us**.

#### 8. Mergers and acquisitions

If **you** acquire an entity during the **period of the policy** whose annual revenue does not exceed 20% of the **company's** annual revenue, as stated in its most recent financial statements, cover is automatically extended under this Policy to include the acquired entity as a **subsidiary**.

If **you** acquire an entity during the **period of the policy** whose annual revenue exceeds 20% of the **company's** annual revenue, as stated in its most recent financial statements, cover is automatically extended under this Policy to include the acquired entity as a **subsidiary** for a period of 45 days.



We will consider providing cover for the acquired entity after the period of 45 days if:

- a. **you** give **us** full details of the entity within 45 days of its acquisition; and
- b. **you** accept any amendment to the terms and conditions of this Policy or agree to pay any additional **premium** required by **us**.

In the event **you** do not comply with a. or b. above, cover will automatically terminate for the entity 45 days after the date of its acquisition.

Cover for any acquired entity is only provided under this Policy for any act, error or omission committed on or after the date of its acquisition.

No cover will be automatically provided under this Policy for any acquired entity:

- a. whose business activities are materially different from **your** business activities;
- b. that has been the subject of any lawsuit, disciplinary action or regulatory investigation in the 3 year period prior to its acquisition; or
- c. that has experienced a **cyber event** in the 3 year period prior to its acquisition, if the **cyber event** cost more than the highest **deductible** of this Policy.

If during the **period of the policy you** consolidate, merge with or are acquired by another entity then all coverage under this Policy will terminate at the date of the consolidation, merger or acquisition unless **we** have issued an endorsement extending coverage, and **you** have agreed to any additional **premium** and terms of coverage required by **us**.

#### 9. Non-renewal

If **we** decline to renew this Policy, **we** will send **you** written notice by registered mail to **your** last mailing address known to **us** at least 60 days before the expiration date stated in the Declarations page. This written notice will include the reason for non-renewal and proof of mailing will be deemed sufficient proof of notice.

#### 10. Our rights of recovery

**You** must maintain all of **your** rights of recovery against any **third party** and make these available to **us** where possible.

**We** will not exercise any rights of recovery against any **employee**, unless this is in respect of any fraudulent or dishonest acts or omissions as proven by final adjudication, arbitral tribunal or written admission by the **employee**.

Any recoveries will be applied in proportion to the amounts paid by **you** and **us**.

#### 11. Prior subsidiaries

Should an entity cease to be a **subsidiary** after the **effective date**, cover in respect of the entity will continue as if it was still a **subsidiary** during the **period of the policy**, but only in respect of an act, error, omission or event occurring prior to the date that it ceased to be a **subsidiary**.

## 12. Process for paying privacy breach notification costs

Any **privacy breach** notification transmitted by **you** or on **your** behalf must be done with **our** prior written consent. **We** will ensure that notification is compliant with any legal or regulatory requirements and contractual obligations. No offer must be made for financial incentives, gifts, coupons, credits or services unless with **our** prior written consent which will only be provided if the offer is commensurate with the risk of harm.

**We** will not be liable for any portion of the costs **you** incur under **INSURING CLAUSE 1 (SECTION E only)** that exceed the costs that **you** would have incurred had **you** gained **our** prior written consent. In the absence of **our** prior written consent **we** will only be liable to pay **you** the equivalent cost of a notification made using the most cost effective means permissible under the governing law.

## 13. Supply chain interruption events

In respect of **INSURING CLAUSE 3 (SECTION C only)**, it is a condition precedent to liability under this Policy that **you** submit to **us** a written report from the **supply chain partner** confirming the root cause and length of the outage.

## 14. Verification of fund transfers

In respect of **INSURING CLAUSE 2**:

- a. **you** must have in place a **funds transfer policy**;
- b. every **employee** that is authorized to perform or instruct funds transfers on behalf of the **company** must receive suitable training on the **funds transfer policy** within 60 days of the **effective date** and every subsequent 6 months; and
- c. **you** must keep a record of the date each **employee** completes the training stated in b. above and provide this record to **us** on **our** request.

## 15. Choice of law

In the event of a dispute between **you** and **us** regarding this Policy, the dispute will be governed by the laws of the State of the United States of America that the company named as the Insured in the Declarations page is domiciled. **We** agree, at **your** request, to submit to the jurisdiction of a court of competent jurisdiction within the United States of America.

Nothing in this Condition constitutes or should be understood to constitute a waiver of **our** rights to commence an action in any court of competent jurisdiction in the United States of America, to move an action to a United States District Court, or to seek a transfer of a case to another court as permitted by the laws of the United States of America or the laws of any State of the United States of America.